

DIGITAL SERVICES FOR EUROPE

PRACTICAL STRATEGY TOWARDS CITIZEN-CENTERED SERVICES

PROMOTED BY



Urban Agenda of the EU



European Commission



City of Hamburg



The Association of Netherlands Municipalities



Republic of Estonia



Republic of Croatia



City of Split, *Republic of Croatia*



City of Kutina, *Republic of Croatia*



TABLE OF CONTENTS

Introduction	5
Why you need a strategy on digital services	6
• Europe on the global stage	6
• A framework supporting European diversity	6
• Digital services as accelerator	6
Towards a modular strategy	7
• A multi-tiered approach	7
• Definition and execution	8
Building blocks	9
• Awareness	10
• Leadership	12
• Principles	14
• Legislation	16
• Service Portfolio	19
• Procurement	23
• Technology	27
• Incentives	30
• Trust framework	32
From building blocks towards a dynamic modular strategy	35
• Determining your starting point	35
• Creating your local roadmap	35
Appendices	36
• Appendix: background of Leadership building block	37
• Appendix: background of Principles building block	39
• Appendix: background of Legislation building block	40
• Appendix: background of Technology building block	42
• Appendix: background of Trust Framework building block	47
• Appendix: background of Procurement building block	48

Index

SUMMARY

Digital Services for Europe is a practical strategy-building toolkit that helps ministers, mayors and directors (Chief Digital Officers and Chief Executive Officers) of municipalities and EU Member States to move towards a social and technical roadmap for digital services for all its citizens, in which collaboration at all levels of government and private sector are further enabled. It aims at realizing user-friendly and cost-effective services that are citizen-centered, where people have insight into and control over their data.

The toolkit brings good-practices from across the EU together into concrete steps that you can take towards an ecosystem for the development and implementation of citizen-centric digital services, starting today. Digital Services for Europe consists of multiple instruments, that offer knowledge, insight and applicability:

- A set of building blocks that, together, cover all aspects of an ecosystem for citizen-centered digital services and essentially are the components of the modular strategy;*
- A survey through which municipalities and Member States can determine their current position, as a starting point from which they can build their strategy;*
- An dynamic roadmap tool that uses the survey results to provide a local-context roadmap for the elements and implementation steps for Member States and municipalities to move forward.*

The strategy combines technical as well as social aspects, and addresses these from both a political and an organizational perspective. Go to <https://www.digitalservicesfor.eu> to get started on building your own strategy!



Within the Urban Agenda for the EU, the partnership for Digital Transition has developed an action plan¹ to address the impact of the digital transformation within cities. The action plan focuses on the impact of technology on society, and how cities can cope with current and future challenges, regarding urbanization, sustainability and the resilience of cities of the future.

The possibilities of technology are endless. Safeguarding the public interest is one of the main reasons for cities to grow towards a proactive role in this societal change, putting their citizens first. The European Union emphasizes an approach in which technology is citizen-driven and embraces ethical guidelines for future development.

Digital services can help people within cities and rural areas, referred to as “municipalities” from here onwards, to live their lives in comfort and offer support to remain healthy, gain knowledge, work, travel, save time and have fun. Currently many governments only provide a limited number of digital services for citizens, and many challenges still remain. Most services are either only local or national in scale, creating a diverse landscape, incompatibility issues and offering limited scalability, particularly at a European level.

The biggest challenge is to free data from silos and enable data to move to work towards generic services that do justice to people’s needs and diversity, using Europe’s diversity as a strength through coherence. Bringing it all together requires a social and technical framework that supports this aim.

1] https://ec.europa.eu/futurium/en/system/files/ged/digital_transition_action_plan_for_dgum_300818_final.pdf



WHY YOU NEED A STRATEGY ON DIGITAL SERVICES

Europe on the global stage

The impact of the digital transformation on society and the lives of people is enormous. While it brings many advantages, felt in everyday life as an increase in ease-of-living, it also brings an imbalance between nations and companies across the globe. This is because new technology is developing at an unprecedented speed and does not look at national borders, cultures and history.

In recent decades, a small number of large tech-corporations have been leading the way. But the current winner-takes-all markets benefit only a few, rather than many. Therefore, a more balanced and inclusive model is needed for sustainable growth, in which everybody benefits.

Europe can be a countervailing power on the global stage, if we are able to create an ecosystem in which every person in every municipality and country has a role to play, feels included, sees their privacy respected and their opportunities improved.

A framework supporting European diversity

Just as no two people are the same, no two countries are the same. The European Union is intent on finding ways to enhance collaboration and cooperation on many of the complex challenges that our societies are facing. Especially on those that affect us all, we have strong incentives to work together.

In a society that is more and more influenced and enabled by digital technology, it is important to facilitate the required cooperation on a European scale. Although diversity is one of Europe's strengths, it can also be our weakness. Innovative

solutions can't be implemented across countries because of differences in legislation, technology, priorities, means, and so forth.

Therefore, it is necessary to find a common ground that enhances our ability to elaborate and upscale digital solutions and align these in terms of technology (e.g. interoperability), information (e.g. ontology), and public values (e.g. principles and ethics).

Digital services as accelerator

The urgency to change on a European level is felt everywhere. Challenges and opportunities in information technology, machine learning and artificial intelligence have found their way on the political agenda. But governments and businesses are still organized in silos, trapped in complex and big organizations that lack the proper means to interact effectively and efficiently. They fail to benefit from new possibilities, while also safeguarding public and people's interests.

A framework of digital services helps in the regulation of data ownership and usage, helps to create business opportunities, and helps people get remote access to secure government and commercial services, while making use of a trusted digital identity and channels.

Fortunately, we do not have to reinvent the wheel. Within Europe there are several cities and countries that have taken steps to achieve this, or at least endeavor towards these aims. These practices are brought together in the practical strategy-building toolkit presented here, so that you can start building your own strategy.



TOWARDS A MODULAR STRATEGY

Towards a modular strategy

Digital Services for Europe is a practical strategy-building toolkit that helps ministers, mayors and directors (Chief Digital Officers and Chief Executive Officers) of municipalities and EU Member States to move towards a social and technical roadmap for digital services for all its citizens, in which collaboration at all levels of government and private sector are further enabled. It aims at realizing user-friendly and cost-effective services that are citizen-centered, where people have insight into and control over their data.

The complexity of modern society doesn't allow for any linear approach to achieve these long-term goals. In fact, you could argue that when it comes to digital services, current societal dynamics hardly allow for long-term goals with a pre-determined outcome at all, considering that these may well be irrelevant by the time they are delivered.

Based on the practical experience of many European countries and cities alike, such as Estonia, the Netherlands, Hamburg and Croatia, we can however set out to lay a foundation, stone by stone. The practical strategy-building toolkit *Digital Services for Europe* proposed here, provides a number of building blocks that, together, help form an infrastructure and ecosystem for developing and delivering citizen-centered digital services. Some of the building blocks are social in nature while others are of a more technical nature, because a healthy ecosystem is dynamic, diverse and in balance.

The toolkit brings good-practices from across the EU together into concrete steps that you can take towards an ecosystem for the development and implementation of citizen-centric digital services, starting today.

Digital Services for Europe consists of multiple instruments, that offer knowledge, insight and applicability:

- A set of building blocks that, together, cover all aspects of an ecosystem for citizen-centered digital services and essentially are the components of the modular strategy;
- A survey through which municipalities and Member States can determine their current position, as a starting point from which they can build their strategy;
- An dynamic roadmap tool that uses the survey results to provide a local-context roadmap for the elements and implementation steps for Member States and municipalities to move forward.

The modular nature of the dynamic roadmap tool allows for the elements within the building blocks to evolve over time. New elements may be added, while others are updated or removed. Because there is no single approach towards realizing *Digital Services for Europe*, the strategy-building toolkit and the instruments it provides isn't ever 'done'. It rather is based on same permanent beta-principle that is slowly making its way in the modus operandi of governmental organizations.

A multi-tiered approach

Each of the blocks offers specific points of focus for each level of government in the current context; in this case the EU-, national- and municipal-level. Bringing these different levels together, helps to show the importance of collaboration and alignment between actions needed to be taken at each level, making it a combined effort. In this context the national level is twofold: it encompasses actions to be undertaken by the national government and/or actions to be undertaken by a collective of municipalities organized at a national level (in the latter case referring to the scope of the effort, rather than the formally responsible government body).

In general, offering solutions at an EU-level can help create generic solutions at a national and municipal level, due to its cascading effect. Likewise, when able to resolve issues at a national level, this can benefit municipalities to speed up their process of digital transformation.

Conversely, taking action at a municipal level not only allows for validation of national and EU-level initiatives. It also allows for the direct involvement of citizens and the evaluation of user experience. Furthermore, it can provide a trigger for national- and EU-level governments to determine a suitable course and take action in accordance with local practices, creating a bottom-up push that helps bring local practices and European policies or support programs together.

The biggest challenge for the former "top-down" (if you will) approach, is to make sure that policies and regulations are practicable and feasible during implementation and execution. The main challenge for the latter ("bottom-up") approach, is to ensure that developments are in alignment with each other, especially in terms of compatibility of the service-technology and data involved, but also in timing and policy-related decisions on a local scale.



TOWARDS A MODULAR STRATEGY

Fortunately, many cities and countries have formed alliances in facing the challenges together, sharing knowledge and co-creating solutions. Furthermore, the results of the digital survey included in this toolkit help create an overview of existing diversity as well as provide opportunities to collaborate. In the end, a continuous synergy of bottom-up and top-down initiatives, with horizontal alignment to turn our diversity into a strength, offers the best chances of sustainable results.

Definition and execution

In order to provide a practical applicability for the modular strategy components, the building blocks contain a set of “definition elements” and/or “execution elements”. The

definition elements offer the content-focused strategic components (what needs to be in place), whereas the execution-type elements offer the process-based strategic components (how this could be achieved). Together they help lay the foundation for the technical and social infrastructure needed as part of the ecosystem.

For both the definition and execution elements in the strategic building blocks, a number of practical implementation steps is provided in the roadmap at each relevant level of application. Because the implementation steps can be updated and enriched regularly they are omitted from this document, but are included in the roadmap that you can generate using the Dynamic Roadmap tool.

AWARENESS		LEVEL OF APPLICATION		
ELEMENTS	EU-LEVEL	NATIONAL LEVEL	LOCAL LEVEL	
Invest in awareness		Organize local-national collaboration alliances	<ul style="list-style-type: none"> • Assign a trend-watcher] • Organize network events • Collaborate with knowledge partners • Analyze the (local) ecosystem of innovative startups 	

INCENTIVES		LEVEL OF APPLICATION		
ELEMENTS	EU-LEVEL	NATIONAL LEVEL	LOCAL LEVEL	
Emphasize on user-friendliness to stimulate adoption of digital services	<ul style="list-style-type: none"> • Promote user-centricity principles to Member States 	<ul style="list-style-type: none"> • Provide central low-code UX-technology for uniform UX-template • Develop a national curriculum digital illiteracy 	Implement UX technology on local services <ul style="list-style-type: none"> • Organize digital centers in public buildings, offering personal support • Perform user-satisfaction surveys regularly 	

In the “Building blocks” section, each of the strategic building blocks and the elements they consist of are described.

BUILDING BLOCKS

The strategy-building toolkit consists of 9 building blocks. Each building block delivers a part of the ecosystem required to build and implement digital services. In order to be successful, it needs to be applied to the applicable context, as explained in the section introducing the modular approach. The deliverables of each the building blocks is different. This ranges from technological specifications to white label legislation, and from practical tips & tricks to social interventions.

The building blocks are:



Awareness



Leadership



Principles



Legislation



Service portfolio



Procurement



Technology



Incentives



Trust Framework

Although each block addresses a particular aspect of the ecosystem in itself, they are connected as part of the ecosystem as a whole. It is the combination of these factors that allows for sustainable changes in culture and technology; both of which are required on the path to citizen-centered digital services.

Each of these building blocks and the elements they contain, will be explained in their own sections. For each of the building blocks, the main challenge, a possible solution, and the elements to be implemented to develop that part of the ecosystem, is provided².

Dependencies may exist between elements of the different building blocks, or on different levels of government for the same element within the same building block. For example, if no funding programs are provided on an EU- or national level, municipalities can't apply for them. These dependencies need to be identified and, where applicable, incorporated in the analyses of the dynamic roadmap tool, to allow for a smooth transition between the stages of development of the ecosystem and coherence between the levels of government.

²] In case you want more background information on the building blocks, please also refer to the Appendices



Awareness

The drive towards citizen-centered digital services requires awareness at all levels of government. Where commonly shared principles are our guidelines, awareness is our compass. It helps us develop services that are aligned to the needs of social, ecological and economical context in which they are delivered. We also require awareness to determine whether the choices that we make along the way are in line with our principles and reflect the needs of the people in our society. Awareness also helps us refine and retune our principles as we progress.

What's the challenge?

If you are not aware that you have a problem, you are not going to look for a solution. Awareness of the impact and the potential of new technologies to improve the quality of life of citizens and society, can't be taken for granted. In the last couple of years, the impact is becoming more and more visible, and political awareness is growing. New technological innovations and societal challenges are on the daily news. As a result, people are more aware, demand more transparency and expect the same seamless services from the government that they are used to from companies. But in order to change, you need a driving force to address the issue. Whereas new opportunities provide a strong pull, experiencing political, economic or social discomfort can function as a push. In terms of awareness, becoming aware of the problem is part of the solution.

What's the solution?

Looking at the impact of digital transformation, there are several societal challenges that, once aware of them, can function as driving forces.

Waves of disruption – learning to ride the waves

The impact of the digital transformation is enormous: the worldwide market value of data is, since 2018, higher than the oil market. Accelerated by new connectivity (5G) and emerging technologies, it has become a new instrument for countries and companies to secure their position in this new digital era. Its ubiquitous character gives it enough force to change the balance of power in the world.

Moreover, technology is developing so rapidly that the importance of safeguarding human and public values in technology is crucial. We need to focus our efforts on a society that we actually want to live in, and make sure that technology

contributes to this. The waves of technological advancement will be there, whether we are ready for them or not. We should start learning how to ride them, also in the government sector, and to move in the direction where we want our society to go.

Climate change – towards a sustainable world

We use of the capacity of the earth manifold. The effects become more visible every day and might turn out to be irreversible. It destroys our natural resources for future generations to come. If we really want to be able to comply with the Sustainable Development Goals set by the United Nations, we will have to come up with a different framework of thinking worldwide; from economic growth to a resource-based economy with norms and values of the global citizen.

Digital services can help reduce our ecological footprint, for example by taking away the necessity to commute to work or to service providers and by reducing paper documents in our government processes. But more importantly, we need to revisit our digital strategies with the main goal of making cities climate-friendly, circular as well as more agreeable with the use of digital technology for the benefit of its inhabitants and business, with an understanding of systemic effects of this transformation.

Too complex to change – or innovative power

Governments and businesses throughout Europe spend billions on IT investments, hours in expertise and implementation and we have 1000+ products and even more processes. But are we effective in our delivery of services that meet people's expectations?

Our systems have become too complex. We tend to say that citizens are lost in the system, but one could argue that it's the government that is lost in its own complexity. It seems



that we don't have the capacity or means to change this situation.

A different perspective might help. A perspective in which the government has an important role to play. And is able to do so. We might as well be the most innovative organization in the world if we consider that, effectively, we have billions a year in (tax) revenues, billions in working-hours per year, a 100% 'customer' base, as well as an external ecosystem of institutions that can increase our impact greatly. Especially, when combined with the power of public procurement that can stimulate an innovative and sustainable market.

Does the development and implementation of people-centered Digital Services for Europe still seem too great a challenge from such a perspective?

Technology vs. humans – Technology & humans

Many recent societal changes are related to the rapid development and digitalization of emerging technologies. We see more and more potential, but also become increasingly aware of the downside. We need to consider how we develop new technologies in such a way that it adds to people's well-being.

The speed and impact of technological change will not stay the same. In upcoming years, it will accelerate even more

because of emerging technologies such as artificial intelligence (AI), photonics and cognitive computing. These technologies force us to consider how we as humans interact with technology and what ethical issues we foresee in the future. This asks for an ethical and societal framework when applying these technologies in the development of digital solutions.

My data – My value

At the time of writing, the combined value of Google, Amazon, Facebook, Apple and Microsoft is above \$3 trillion, mostly profiting from advertising revenues targeted to our online behavior. The corporations provide the platforms, while their users provide the content that actually makes them valuable. If the value of these platforms is so dependent on its users to be of value, shouldn't digital platforms be paying their users, as well as giving full ownership of their own data?

Awareness Toolkit

It is hard to grasp the impact and implications of the digital transformation. That is, until it disrupts your organization or even our entire society. It therefore requires a conscious effort to create a sense of urgency and awareness.

Strategic building-block elements

In order to become aware, there are several elements which you can include as part of your strategy:

NR	ELEMENT	INTENDED RESULT
1	Invest in Awareness	A continuous effort is made to stay up to date on political and technological developments
2	Setting the agenda	The ability to address issues concerning the impact of the digital transition is organized structurally
3	Strategic narrative	The digital transition is a center-stage topic on the political agenda
4	Incorporate social value in the core of business models	Business models and business cases include and emphasize society-driven growth aspects, rather than only profit-driven growth, and balance the benefit of the few with the benefits for all.
5	Sense of urgency	The follow-up and implementation of desired change(s) set in motion by the introduction of new legislation, principles, technology, etc is actively pursued and enforced.
6	Create means and opportunity	The willingness and ability to change in response to challenges that are part of the digital transition are supported



Leadership

Developing, implementing and (re)using government service(component)s, requires digital leadership to focus our actions and ensure collective effort. Intrinsic motivation to create citizen-centered services needs to be supported by a thorough understanding of technological possibilities and implications.

What's the challenge?

Although everything starts with awareness, leadership is necessary in order to actually make a change. Leadership needs to give focus and create conditions for any movement or organization to become adaptive and yield desirable results.

An organization must be adaptive when confronted with modern digital technologies. The technology must be identified, understood, applied reasonably and incorporated in new business models. It is widely assumed that these technologies will significantly and inevitably disrupt the public sector as we know it. While private businesses are confronted with a choice of either adapting to innovative business models or disappearing, the public sector has never been subject to market forces and is therefore not known for a high level of adaptivity. In that respect, it is understandable that top executives might fail to realize how such new technologies could benefit their sometimes decades-old structures and cultures. However, we can't ignore the pressure from citizens for the government to be more efficient, transparent and flexible as a way to gain trust.

What's the solution?

It is important to become an adaptive organization, city and society and the solution is simple: organize your leadership at all levels.

The requirement to adjust and prepare the organization and the entire government to the forces of digital transition needs to be made clear to the top decision makers. It is essential that the highest levels come aboard, as they are the ones communicating the information, creating awareness on the need for change, and setting the course for the different departments and agencies. The first priority is to become more agile as an organization, otherwise, even if the need for change is felt, there is no way to actually do so.

Of course, the above-mentioned awareness and resulting leadership needs to be introduced at a political level, too. Many countries have by now adopted that philosophy and created dedicated positions for digital leadership both on the local and national level.

Strategic building-block elements

In order to strengthen digital leadership, there are several elements which you can include as part of your strategy:



NR	ELEMENT	INTENDED RESULT
1	Digitalization challenges and solutions are boardroom decisions	Information technology is considered a strategic topic that is managed and/or monitored by the board of directors directly.
2	Organize multi-layered leadership	Each level of government has their own responsibilities and challenges, but those are not restricted to that level; initiatives undertaken at each level are in line with broader challenges and in support of offering a sustainable solution, rather than being isolated or even counterproductive
3	Organize mandate over implementation and validation of principles, legislation and digital services	A formalized institution/board/platform that supervises the implementation and the compliance with common standards and other services is installed
4	Define vision, values and principles of the adaptive organization	Together with your leadership, the vision, values and principles of the adaptive organization to prepare your organization for dealing with rapid developments by increased agility have been defined
5	Strategic Portfolio Management	The IT-portfolio has been made part of the business portfolio, thereby aligning prioritized societal challenges relating to the primary responsibilities of the government with possible investments in enabling technologies, process optimization and standardization
6	Vision to strategy	The link between regional identity and vision on the one hand, and marketing and communication on the other hand has been created
7	Create enabling conditions	Conditions are created (e.g. funding and mandate) that help attract the right talent (personnel), implement new legislation, procure modern technology, etc required for the digital transition and -services
8	Tactical Leadership	Tactical leadership to translate strategy into operational implementation has been organized
9	Public value is included in business cases and portfolio management criteria	Profit management, including positive social and ecological impact by determining which digital services will have the most impact in improving quality of life and decreasing societal costs, has been organized
10	Prepare legislative framework for enabling digital services	The legal framework has been brought up to the level required for modern digital services (see legislation building block), and required legal changes have been made



Principles

User-centricity of services greatly improves when developed along certain guidelines. In a world of (technological) options and decisions to be made at each step of the way, principles function as our guides. They form our proto-strategy; not to plot the outline of our course, but aiding us in implementing public values in our technology and the development of European government services. These principles concern the use of data, technology and social conduct.

What's the challenge?

To provide focus and direction in developing a strategy towards digital services, principles should be in place as guidance in the decision-making process. Over the last years, several declarations have been released on a European scale that bring us a number of important principles. These are both technical and social in nature, offering a broad basis for developing a European strategy for municipalities and countries alike.

Unfortunately, even though declarations have received wide support, the principles themselves are still not well known and/or embedded in government strategies and implementation plans or strategic European programs. The main challenge is finding methods to translate them in suitable courses of action to implement them in both the development process and in the use of the services.

What's the solution?

The principles form the basis of the strategy. All other building blocks rely on these principles one way or another. The principles on eGovernment are already in place and signed by all ministers in Europe. But the challenge is to apply these principles on a local level and to translate them to your specific local needs and context, so they create value for citizens. This building block translates the principles described in the ministerial declaration on eGovernment into the value proposition for the citizens and cities. It also describes how these principles can be applied in the system to ensure that they are executed. The 'Join, Boost, Sustain' declaration, that was launched in December 2019, includes a number of

principles that further help anchor our common effort:

- A citizen-centric approach;
- A city-led approach at EU level;
- The city as a citizen-driven and open innovation ecosystem;
- Ethical and socially responsible access, use, sharing and management of data;
- Technologies as key enablers;
- Interoperable digital platforms based on open standards and technical specifications, Application Programming Interfaces (APIs) and shared data models.

The value proposition

It is important to bring these principles back to the lives and living environment of the people. These are the principles translated into the value proposition to citizens on how you can deliver digital services as a city:

My life, our community

- You can, where and whenever you want, take care of the things in life you need.
- You decide who you share your data with
- The value of the data comes back to you
- The system works for you, not the other way around
- Plug and play, it's inclusive
- You get time for the important things in life

Strategic building-block elements

The values mentioned above are translated into and support by the following principle elements which you can include as part of your strategy:



NR	ELEMENT	INTENDED RESULT
1	Once-only principle	The principle that data that has been entered once shall be used for further use and not be required to enter again is in place and actively monitored and enforced in all relevant processes and applications
2	Digital-by-default	All government services are also available digitally, in user-friendly user stories
3	Trustworthiness and Security	The digital systems used by your government, comply with the highest standards in terms of (data) security, ensuring that data is safe and cannot be abused
4	Openness and Transparency	Users know what the government knows about them, which data is used where and by whom and no data is used without the user's consent or legal grounds'
5	Interoperability by default (between sectors)	Data the user has entered for one government entity is transferable to others based on portability, interoperability and data standards, in compliance with GDPR-regulations; so when a citizen moves to another (part of the) country, her/his data will move with her/him and be available and accessible there, too.
6	Data Commons for public data ownership	Data principles are in place that ensure that data is available to the public whenever applicable (e.g. compliant with privacy regulations, etc)
7	Citizen-centric design; for and with the user	Digital Services are designed for and with the users, incorporating user input in the development and implementation process
8	No legacy-principle	A no-legacy principle is in place, allowing for active and timely replacement of software before it reaches end-of-life for support or outdated (security) standards.

See the 'Appendix: background of Principles building block' for further elaboration on this building block.



Legislation

To be able to maintain a steady course and mark important decisions, legislation helps solidify government policy at key points along the way. It is also a vital enabler for introducing and implementing various aspects of digital society and the government services it embodies. This includes a translation of ethical principles in the design and use of digital technology and agreement upon a mutually desirable code of conduct.

What's the challenge?

European legislation

Within Europe, we have legislation that lays the basis for the European approach to digital services. All Member States and cities need to be compliant, which creates an urgency to apply digital service-guidelines. The most important EU legislation and directives for the digital transformation are:

- General Data Protection Regulation (GDPR)³
- Electronic Identification and trust services for electronic transactions (eIDAS) ⁴
- Payment service directive (PSD2)⁵
- Single Digital Gateway Regulation (SDGR)⁶
- Open Data Directive (ODD)⁷
- Coordinated Plan on Artificial Intelligence (CPAI)⁸
- Digital Service Act⁹

What legislation do you need on a national level?

Next to the European legislation, individual countries need to integrate certain directives within existing or new legislation to ensure that the basic principles are implemented in the system. This instrument helps countries to set the boundaries, and to act if compliancy is inadequate (high trust, high penalty).

To get legislation in place will be difficult and complex. It needs leadership of a minister with mandate who directly reports to the prime minister. Often it is the minister

of internal affairs or the minister of finance, but which specific position depends on the country.

In general, effective digital governance does not necessarily require a large set of new specialized legislation. A step-by-step approach to establishing the legal basis is to analyze existing legislation and identify gaps where law may pose obstacles to the development of digital governance. Aspects necessary for enabling the provision of digital services can be added into relevant existing legal acts.

As an alternative to the approach of adjusting existing legislation step-by-step to create a legal basis for the digital infrastructure, it is also possible to work towards an overall "digital infrastructure law". Position this as the law which is the enabler for the digital infrastructure of the country and make it applicable for all. Other (sectoral) and directives need to be (made) compliant with this law. In order for this to work, the digital infrastructure law needs to concern only the key enabling factors to keep the impact on existing legislation as small as possible.

In either case, over-regulation should be avoided. Too many regulations might create a parallel system of governance and lock-in technologies. Locking-in the use of any specific technologies should be avoided at any cost as this would hamper the future development of any services, or the possibility to easily replace existing technology by a more advanced one. Legal expertise should be engaged early in the process of digitizing the services.

3] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

4] https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf

5] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

6] https://ec.europa.eu/growth/single-market/single-digital-gateway_en

7] <https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information>

8] <https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence>

9] <https://ec.europa.eu/digital-single-market/en/new-eu-rules-e-commerce> (under development, see bottom)



What's the solution?

There are a number of primary areas that need to be addressed in order to set up a legal basis for a digital infrastructure. The legislation toolkit for nations below, contains the core elements:

- Digital identity documents act
- Digital signatures act
- Public information act
- Personal data protection act
- Open, closed and AI act.

Digital infrastructure law

The more legislation you have, the less chance there will be that you can implement it successfully. The European Union can play an important part in setting up the outlines for legislation relating to the digital infrastructure at a European and national level, including data-protection, interoperability and access to public information. Implementation at a national level is however greatly enhanced if a legal basis already exists, giving legality to digital signatures, establishing an interoperability layer, etc.

But the bottlenecks are the legal acts and directives on the national and local level that are interdependent and sometimes even contradictory. Create insight in the existing legislation (on both levels) and check if they are aligned, compliant and update if necessary.

Like stated in the beginning; the digital transformation is a cultural change. You need to be aware that laws and directives are interpreted by people. Translating the “meaning” of the law into a story for citizens and lawyers, policymakers, etc., is key to keep interpretations aligned.

Bottom-up legislation

But we are in the middle of a digital transformation. This means every day new technology gets released to the market. If drones and robots will be the delivery service of tomorrow; what needs to be in place to secure privacy, security and public values? There is a need for legislation that is simple and adaptive.

But there are two bottlenecks:

- The procedure of creating new or adapting existing legislation takes too much time, because it depends on a lot of human interaction and we don't start from a greenfield situation. It is the strength of our diversity in Europe and our democratic value. But it is too slow to keep up with the speed at which new technology, and challenges, emerges.
- The validation of legislation works through our democratic process of voting, as well as a more continuous citizen engagement. But applying legislation as it is meant to be works differently in real life. The voice of the people is much less heard as it could be. We still need political leaders, but the validation on how laws and directives are executed need to be improved to ensure that legislation is applied and understood.

The solution lies within digitalization of the democratic process. Because of the digital transformation we have the instruments to work on the validation of legislation with input of the crowd. First step is to enable people to vote and make them real time part of the democratic process. This way we secure the most important aspect of our democratic values; validation and dialogue. This makes it much easier to update legislation and become adaptive.

Bottom-up legislation needs to be combined with the European and National legislation, to ensure coherence. The combination of the top-down and bottom-up approach will form the perfect balance for simple and adaptive legislation.

What steps do you need to take?

1. Analyze the current legislations on national level
2. Define the strategy and content (based on the white labels) on the “digital infrastructure law”
3. Adjust the procedure of adopting legislation
4. Define the strategy for bottom-up legislation and democracy
5. Define the 5 icon projects to test the strategy and legislation
6. Define the deadline to start
7. Monitor and punish (as change mechanism)



Strategic building-block elements

The following legislation is essential for delivering citizen-centric digital services, to be included as elements of your strategy:

NR	ELEMENT	INTENDED RESULT
1	Digital ID regulated in legislation	A secure form of online identification - digital identity - which allows people to electronically authenticate themselves towards a government, essential for using e-services, has been established legally
2	Valid digital signature	A legally binding digital signature is in place, allowing for processes and procedures to be executed digitally in their entirety, including formal validation of documents, signing contracts and decision making
3	Legal basis digital portal	A single digital gateway as the primary access point to public information, public services, and to public electronic services gives citizens a single point of access to their government and the services it provides has been established legally
4	Legal basis for data repositories	A law has been established ensuring that a data repository of a public authority is a digital database, and setting out requirements for such databases, giving legal basis for digitalizing all data repositories managed by the national and local government.
5	Digital Services Act	A law stating that public services must be made available for citizens also digitally has been established, enforcing the implementation of digital-by-default principle
6	Cross-border interoperability	Compliance with the Single Digital Gateway Regulation, ensuring cross-border interoperability between different EU member enabling citizens to use their data across borders, is actively enforced
7	Legal basis for exchange layer	A law that states that data must be stored digitally and always re-used is in place, providing legal basis to establish a data-exchange layer through which data can be moved to/from the data repositories.
8	Prohibition to ask same data twice	Legal prohibition of public authorities to ask the same data twice from citizens and companies has been established, providing a driving force for digitalising data repositories and building a data-exchange layer, and enforcing the implementation of once-only principle.
9	Enforce digital storage of data	A law stating that all data which the public sector collects must be stored digitally, is in place, enforcing all levels of government to digitalise their data -collection, -processing and -storage procedures

See the 'Appendix: background of Legislation building block' for further elaboration on legislation.



Service portfolio

Whereas principles, procurement and incentives focus on the ‘how’ and the ‘why’ in regard to the digital services strategy, the service portfolio focuses particularly on the ‘what’-question. The number of services provided by the government is enormous, so it is important to decide on which services to focus (first) and how to gradually work towards a complete service portfolio that cover the life-events and needs in people’s lives.

What’s the challenge?

The government offers a wide range of services, most of which can be digitalized. In fact, with a ‘digital first’-policy in place, ultimately all public services will become available digitally, on top of any existing analogue counterpart. For politicians it’s important to realize that an investment is needed to achieve this, even if citizens don’t always directly experience the benefits because services are fully automated, making them hardly noticeable, or because they help run processes in the background. In many government organizations, the IT-portfolio is still often managed separately from the business portfolio, making both less effective because political priorities and technological possibilities fail to meet.

The challenge is to determine where to start and what approach to take towards a roadmap of services to develop, procure and/or implement. There are a number of perspectives that can help make a decision.

What’s the solution?

Public and private services that create impact

In terms of cost effectiveness, there are two main criteria to decide in what to invest; (1) what services do citizens use every day and (2) which services cost society (or your city) the most? The rest can be done later.

Based on the first criterion, it’s important to understand that 90% of the daily digital transactions of citizens are business-related (banking, food, mobility, etc.). In terms of government services, only 1% to 5% of the population has more than one government product that they use on a regular basis (per year). Around 10-15% of the population receives services of the local government. The rest of the population uses the services once in a few years (e.g. obtaining a new passport, driver’s license, etc).

In order to be successful, the strategy for digital services therefore should be a cooperation between government and business. This way people frequently have the ability to familiarize themselves with the services, as well as to provide feedback. Therefore, your strategy should include both public and private participation. The role of the government should at least be to safeguard the public interest and to secure the digital infrastructure (including digital identity).

By working together with businesses, governments are able to add more value to the quality of services and reduce costs dramatically. Analyzing which services claim 80% of the budget, shows where we can add the most value. For example, a labor-intensive procedure that can easily be digitized for most clients.

Lastly, the Digital Single Gateway Regulation lists a number of specific cross-border digital services that must be made available through the platform, making those a high priority.



Connecting Europe Facilities (CEF) Digital Service Infrastructure Building Blocks

Especially when it comes to cross-border collaboration, the Connecting Europe Facilities Digital Service Infrastructure Building Blocks (CEF Building Blocks) are of importance. They provide a set of readily available services that can be re-used by any public administration in the EU. Among these are:

- eArchiving provides sample specifications, software and support services for describing, transmitting and preserving data based on international standards.
- Big Data Test Infrastructure (BDTI) is a virtual sandbox where public administrations can experiment with different big data tools and techniques to innovate new digital services and solutions.
- Context Broker centralizes and consolidates data from different IoT data sources, enabling comprehensive analyses and real-time reports for more informed decision making.
- eDelivery offers specifications, sample software and support services for setting up a registered delivery service infrastructure for exchanging data and documents.
- eID helps to set up the technical infrastructure needed to electronically identify citizens, businesses and public authorities from other European Member States, as defined in the eIDAS Regulation.
- eInvoicing supports the seamless generation, sending, receiving and processing of electronic invoices across borders in line with the European Directive and standard on electronic invoicing.
- eSignature helps to create and verify electronic signatures in line with the eIDAS Regulation.
- eTranslation provides machine translation services that can be used on demand for translating text snippets and documents (web service), or integrated directly into a digital service platform.
- European Blockchain Services Infrastructure (EBSI) to enhance trust between parties and improve the efficiency of operations
- Once Only Principle (OOP) reduces administrative burden for individuals and businesses. The OOP is currently a CEF preparatory action.

The question instead of the product

What the business sector realized already for a very long time is that the services they deliver are based on the need of the customer and not the product that they sell. Within the government most of the time we still “sell” the product. The transformation that is needed is to turn this around; the solutions should be citizen-centered and based on the actual needs.

Within Europe we see differences in culture and different patterns in the way people live. But at the end of the day we are all human. After analyzing the services within Europe and worldwide you see that 80-90% are identical across the globe. The details may differ, but in every country people pay taxes, get married, have children, work or receive government support, go to school. The experiences from Estonia show that there are around 3000 government services (of which 98% is digitized). Interesting fact is that for India it's a very similar number. Even though the countries differ in size (1 million vs. 1 billion inhabitants) the number of services is roughly the same. The solution is to focus on the common, build it and implement it.

Build trust; service by service

Change always creates friction and the trust in the government as a service provider is generally not high. Transparent solutions that work seamlessly, help to make your life easier and build trust. Service by service you need to implement new facilities in a safe and secure way. Selecting services that people actually use frequently, helps people familiarize themselves with them, as mentioned earlier.

The roadmap of digital services should start small with a simple service that can be tested on security, customer experience, effectiveness and privacy. If it works and is well received, the next service is one that might be more complex and touch all citizens. Within government services, declaration of taxes is one which is interesting to implement early on, because of the high volume (in people) and level of standardization. Next step is to include business services that will increase the frequency of usage even more. After that it's a matter of regularly adding new services to keep people involved.

The implementation of eHealth asks for extra attention.



Medical data is particularly sensitive, and security and trust are of paramount importance. The timing of adding such services shouldn't be too early in the process. Build trust by showing the benefits and proper delivery of other services first.

The top 10

The following list offers a top 10 of services to implement consecutively in order to build trust, by balancing impact and volume:

1. Digital identity (population registry) - insight and control over your information
 2. Public transport
 3. Taxes
 4. Banking
 5. Citizen engagement (e.g. polls or voting)
 6. Smart Grid
 7. Being an entrepreneur
 8. e-Health
 9. e-Prescription
 10. Other local politically relevant service(s)
-

Impact of the service roadmap

New technology allows the use of machine-to-machine processes, which will allow for a decrease in manual transactions. Next to that the digital infrastructure will, because of the modular technology, decrease the costs of technology. The impact of this on organizations will be big and decrease the organizational and societal costs. This is a threat for the status quo, but from a political perspective also very interesting because cities can realize exponential cost reductions and improve the quality of life for its citizens. It is however crucial to ensure transparency in dataflows and automated decision-making processes when implementing machine-to-machine transactions.



Strategic building-block elements

In order to develop your service portfolio, the following elements can be included in your strategy:

NR	ELEMENT	INTENDED RESULT
1	User stories for life events	For each of the most common life events, user stories have been defined in preparation of designing user-friendly digital services
2	Demand-based product backlog based on user stories	The government backlog for the service portfolio is filled and prioritized based on actual/measured user-demand, rather than the government pushing new services based solely on new technological possibilities.
3	Implement user evaluation methodology to build trust	To secure that services fit the needs of citizens, a validation methodology is in place, which provides feedback on the (quality of the) implementation helps build trust and acceptance
4	Implement service by service	New services are implementend one at a time, starting with those that help address actual societal issues and needs, allowing for a gradual acceptance of digital services by citizens and organizations
5	Public-private collaboration	The service roadmap includes collaboration with and support of private sector services (banks, insurance, energy) as well as public sector services, so that people can get used to using digital services more frequently (because many government services are only used a few times a year or less).
6	Define user stories for future government services	Future services currently not yet part of the government's portfolio (e.g. services or products realting to drones
7	Define technical and functional specs of building service-components	To ensure compatibility, technical definitions of each component in the service portfolio are in place (e.g. for each microservice in component-based architecture), ensuring that for each of the components it is specified what it does functionally and what it requires technically.



Procurement

Procurement is an instrument to ensure that the public interest is safeguarded and allows the government to relate to the market, stimulate innovation and sustainability. Through procurement we have the possibility to make sure that technology is adaptive and to secure the citizen-centered perspective, such as ownership of your own data. It's also an instrument which can enable a more effective way of collaboration between government

What's the challenge?

One of the critical conditions for success of Digital Services for Europe is procurement. If you procure at the right level and the right products, cities are able to use the generic infrastructure. This way costs in execution and services are decreased.

Currently there are several challenges that cities face regarding the procurement of technology:

- In most countries the software is traditionally organized in front, mid- and back offices including the data sources which are provided by IT companies. The IT infrastructure is fragmented in silos. Because of this dependency on the market, cities and countries experience vendor and platform lock-ins which create higher costs and less flexibility.
- Governments need to apply procurement to secure transparency in the market so there is a level playing field. This asks for the right understanding and knowledge within the government to secure the boundaries. Because of the rapid pace of technology most cities do not have this knowledge available.
- Another issue is that the speed of the procedure of procurement is not as fast as technology is developing. Combined with the vendor lock-ins in cities, it is hard for small, innovative companies to enter 'the system' due to complex procedures.
- The last challenge for cities is to transform their digital infrastructure from big solutions towards the modular (micro-)services and engines built on the container technology. In this context, implementing (procuring) open-standard based urban digital platforms is important for interoperable dataflows and to avoid vendor lock-ins. Within the procurement process there needs to be a balance between optimizing the current infrastructure

(re-use which is already there) and develop new adaptive building blocks which are interoperable on the current infrastructure. Defining a transformation plan enables the controlled replacement of existing applications.

See the 'Appendix: background of Procurement building block' for further elaboration on the micro-services, engines and container strategy.

What's the solution?

In line with the 'Technology' building block introduced previously, there needs to be an adaptive and agile procurement strategy. This requires agile procedures and an organization based on principles which help find the balance between innovation and continuity.

The strategy will set the boundaries and create the role for the government as a curator of the platform in which no-legacy policy is one of the main drivers to become adaptive and avoid vendor lock-in and platform lock-in. We define the following solutions:

1. Principles for procurement;
2. The procurement organization;
3. Simple and agile procedures.

Principles for procurement

The characteristics of technology introduced previously, need to be translated to your procurement strategy:

- The role of procurement is to become the curator of the technology platform for cities in order to support government and businesses in developing human driven services.
- The platform is based on agnostic technology, which



means that its functioning is independent from the chosen technologies, in order to make cities adaptive and to secure our technology sovereignty as Europe.

- Data- and platform-ownership are based on European technology to ensure that the data is regulated under European legislation.
- The business model of the microservices is transparent and will cover the basic costs for maintenance, scalable hosting, support and development.
- The Architectural Framework model based on the OASC MIMS in combination with the CEF Building Blocks (see 'Service Portfolio' above) form the boundaries for the procurement strategy.
- Procurement procedures should facilitate established vendors as well as small startups. To create a level playing field;
- No-legacy policy; right from the start, every product within the platform has an end date and will be replaced at the end of the period.

The principles of procurement will have an effect on the role of the IT suppliers. This is due to the fact that the technology will be a commodity based on the platform strategy and the no-legacy policy. There will be opportunities for the market, because micro-services still need to be developed, the hosting (including scalability) needs to be provided, as well as the implementation and support on maintenance; all will be lots that need to be procured. The steering on the strategy will be executed by the independent procurement organization.

The independent procurement organization

The key to success is the execution. The procurement organization is essential to the difference. In order to safeguard the public interest and create a transparent and open market, in which the knowledge and execution power of the market is secured, there needs to be an

independent organization which is a curator of the platform and secures the execution. The steering governance of this agent is crucial. The organization is preferably steered by a multilayered board with the responsible digital department as chair. To secure the knowledge and execution of the businesses and knowledge institutions, a board of advisers is necessary. The board is responsible to provide the steering, resources and budget. The procurement organization is responsible for the following tasks;

- Overview of the technology roadmap
- Execution and implementation of the core framework
- Maintain, secure and audit the principles of procurement
- Execution of the procurement procedure of the components of new technology if applicable
- Execution of the procurement procedure the plots on development, hosting, implementation and support

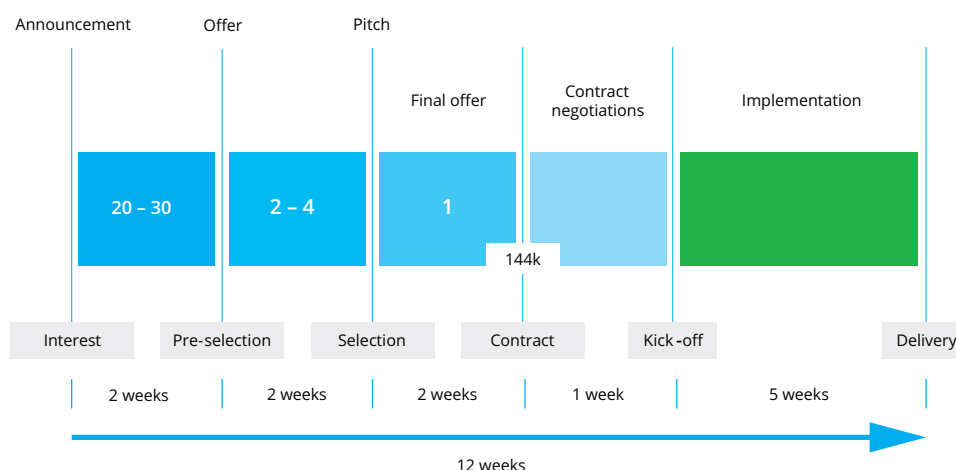
The implementation on a local level is the responsibility of the CDO or CIO with support of the procurement organization.

Simple agile procedures

The strategy for procurement enables a more agile procedure to enable the market to anticipate faster in developing building blocks. The procedure for technology building block is based on the following process.

Within this process the maximum contract is based on the minimum amount which is legally based on European procurement standards. The contract included funding for the development and support for the period of the no-legacy policy. The procedure is executed by the independent procurement organization.

To secure that we develop agnostic technology which is safe, the following checks will be built in in the procedure:





REQUIREMENTS	TOPIC	DESCRIPTION
Technical and architectural principles	API	The API need to apply to the API guidelines as described in the CEF building blocks. The supplier is responsible for building in health checks
	Development	The supplier assures and guarantees the quality of the software based on the set of criteria
	Technology	The software needs to support asynchronous web applications (i.e. AJAX)
Security	Use of open source	Support open source frameworks but needs to have insight in the licenses
	Code	There is a specific list in which the code needs to be compliant
Code	Logging	The logging will go through the standard framework that is used by the procurement organization
	Source code	The source code will be made transparent via a private solution towards the broker
	Delivery	The delivery of the code needs to be able to be translated to the container image by the broker

The requirements give the status at the time of writing but are subject to change, as new technology and methodology become available.



Strategic building-block elements

In order to implement your procurement, the following elements can be included in your strategy:

NR	ELEMENT	INTENDED RESULT
1	Define the responsibility level for procurement	The mandate for the procurement organization have been defined and established, allowing for scoping of the market and developing the procurement strategy in collaboration with technical, legal and policy specialists
2	Define the principles and standards of the procurement strategy	Principles and standards for the procurement strategy (e.g. micro-service based architecture, using open standards, different lots for hosting, updates, support etc) are defined and established through a formalized decision
3	Establish the procurement organization (independent broker) and procedures	An independent procurement organization (broker) is established that monitors compliance with the principles and standards for the procurement strategy
4	Define the transformation path	A transformation path to move from the existing (vendor-locked-in) infrastructure, to an infrastructure procured according to the new procurement principles, standards and strategy is defined, ensuring continuity of business process within the operational infrastructure at all times
5	Execute the procurement strategy	The procurement strategy is actively executed, monitored and evaluated according to the principles and standards
6	Ensure maintenance and deliver support to the end-users (cities)	The procurement organization is in touch with its clients (departments etc) to offer support and ensure maintenance of existing services and anticipation of future services



Technology

Without a technical application of digital services, the rest remains prerequisites. Technology anchors functionality and enables delivery of services in response to people's needs, while in the process ensuring safety, security, flexibility and transparency. As reliant on technology as modern society has become, it is fundamental to its functioning.

What's the challenge?

One of the main reasons that governments and businesses have trouble to be adaptive, which is necessary to become and remain able to deliver proper digital services, is the legacy technology that organizations have in place. Within this legacy, it is often difficult to replace parts of the system, unless it's modular, and the data is often integrated within the application and inaccessible to its users. This means that organizations do not always have access to all the data they use. This creates a vendor lock-in in which the core operation and services are depending on specific external vendors or suppliers.

The second challenge is that data currently is not legally owned by people but by the organization using it to provide their services. This means that people do not (always) have insight into their personal data. Within Europe, the personal-data-management movement is pushing to transform this model to assure that citizens get insight into their own data, as a personal and legal right.

Because of the rapid pace at which technology is developing, it needs to be modular and adaptive (e.g. containerized) and a no-legacy policy should be in place. This enables rapid adjustment and upgrades to the latest technology. The challenge is to develop a digital infrastructure for services that supports this transition.

What's the solution?

An adaptive and transparent infrastructure for offering integrated digital services requires certain elements and principles to be in place:

- The identity based on a unique identifier (of people, objects & organizations) is the core of the technology;
- The data integration layer enables governments and companies to interact with the unique identifier and create transparency, builds trust and gives the owner control over their data and information;
- The interface layers are modular and are adaptive for technology to come; from apps into the era of augmented reality (AR) and virtual reality (VR);
- The data is decentralized and the responsibility of the organization using and maintaining it in their processes leading to the products and services they provide. It is independent from the software which means it is always accessible;
- The government data is available in the cloud through different servers to secure continuity in case of cyber-attacks;
- The software is built up out of micro-services through API's and container technology to become platform-independent to avoid vendor or platform lock-ins. This makes it adaptive and plug-and-play;
- The logic through artificial intelligence (AI) is transparent and explainable. Also, the audit trail is transparent;
- There is a sensing and service layer which forms the core for digital services, not containing (business) logic to enable separation of front-end and back-end for agility in future development and multi-channel approach;
- The footprint, control and security is the responsibility of an independent authority and is automated as much as possible.

10] For a detailed description, see the 'Appendix: background of Procurement building block'

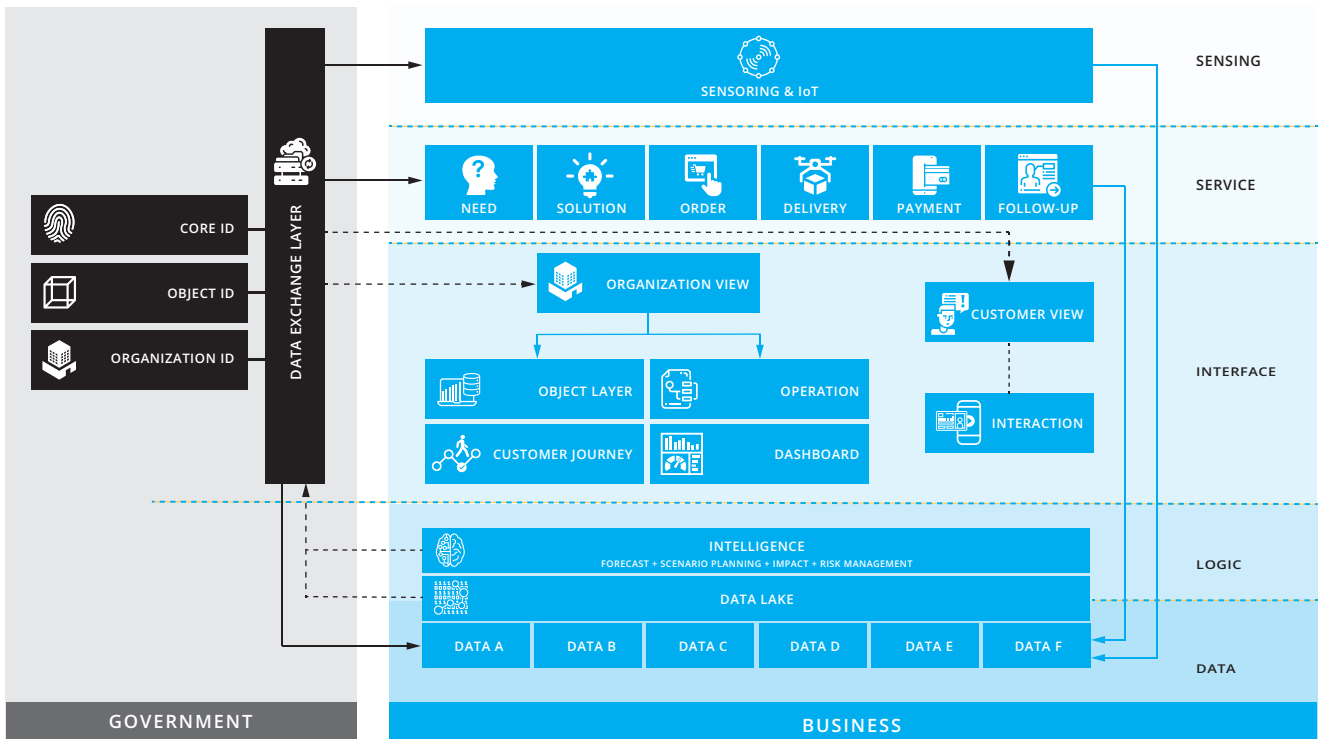


The toolbox

These elements combined provide a toolbox, offering a plug-and-play platform which enables cities and businesses to develop seamless digital services for all European citizens. The role of the government is to act as a curator. This means to set the standard, including ethical principles, and create a playing field for business and governments to develop on. This way we can safeguard the public interest and accountability. For certain components the government should be responsible, such as digital ID and data exchange layer, while others can be developed and maintained up by the market. Below is a graphical representation of the infrastructure:

What steps do you need to take?

1. Define the 'should be' situation as a system architecture and technical architecture, applying the elements of the Principles-building block;
2. Based on the system architecture, map the currently available components (including the testing on interoperability) to define the blank spots;
3. Define the roadmap of transformation to move from 'is' to 'should be' situation, by deciding upon the order in which legacy components will be replaced;
4. Organize in the governance who will steer the transformation;
5. Organize the execution with a 'broker' as an independent curator to execute the implementation of the transformation path;
6. Develop all building blocks as basis for the digital infrastructure of the country;
7. Define the implementation plan to measure the speed of usage of the building blocks and services;
8. Organize the support and maintenance on the digital infrastructure.





Strategic building-block elements

In order to develop your technical infrastructure, the following elements can be included in your strategy:

NR	ELEMENT	INTENDED RESULT
1	Digital Identity	A safe and secure Digital Identity (including a core ID and identification and authentication), based on the European standards (GDPR, eIDAS, PSD2), is technically available for humans, objects, organizations and Artificial Intelligence (AI)
2	Human and sensor interface / interaction	An interface layer based on microservices- and business-engines architecture, enabling the organizations (government and business) to deliver more effective and efficient services to citizens and customer, is available for customer perspectives (from apps to VR/AR solutions) and organization perspectives (operational dashboard, customer journey manager, and object layer (i.e. for digital twins)).
3	Logic Layer	Business processes (including those related to customer need, solution, order, delivery, payment & follow-up) are handled using open standards for process notation, architecturally separated from interface elements and data storage by using a data-exchange layer
4	Data exchange layer	A data-exchange layer is in place, allowing for secure data transactions, citizen control over their data, GDPR-compliance and while allowing data stored in local and national databases to be made accessible, in a simple and standardized manner, to service providers (government and business) to easily and quickly offer digital services to residents and companies
5	Data-services	Data stored in government repositories is made accessible through data-services using open api-standards and information models to ensure interoperability and agility, compliant with GDPR and privacy-by-design principles
6	Digital data repositories	Data-repositories are in place to digitally store government data to be used in business processes, based on data standards and -models for cross-sector use of data in chains of services between service organizations
7	Certification center	A certification center that safeguards legitimate use of government data through technology, legislation and governance is established as part of the technological framework, which handles the intake process for new services to access the digital infrastructure as well as monitoring active services
8	Data-analysis tooling	Data analysis tooling, such data lakes, transparent machine learning tools and visualization tooling, with access to data repositories and compatible with the data exchange layer, is available

See the 'Appendix: background of Technology building block' for further elaboration on technology.



Incentives

New ideas aren't innovations until you apply them, and digital services won't appear spontaneously. That means a certain push or pull is needed to get going and, in doing so, to deliver the quality people should be able to expect. Incentives can be part of your strategy to increase quality of the services as well as increase adoption. It relates strongly to the ethical principles and the service portfolio.

What's the challenge?

Whether you are an employee or a private citizen, the driver for change often is 'what makes life easier for me?' This also has a downside because we live in a world in which individual needs don't necessarily match society's needs. When it comes to digital services, it is therefore important that (ethical) principles are taken into consideration. A community-based and transparent approach, enabling people to participate, leaves room for incentive-based nudging.

Nudging and behavioral science is an instrument that can help to achieve a certain goal. It can be used for 'good' or 'bad', and therefore the intention is essential here, hence the reference to ethics and transparency previously. A key question when defining incentives and nudging is: what's in it for me and for us all?

What's the solution?

In the process of developing the strategy for digital services, the incentive roadmap for citizens and organizations is a key instrument and solution. Incentives stimulate possibilities, positive thinking and offer a perspective on the motivation to the desired change. That's why we need to make explicit decisions on which incentives we use, instead of resorting to implicit choices. The roadmap of the incentives needs to be transparent

for all end-users: citizens, public organizations and businesses.

The use of incentives focuses on organizations and citizens. Within organizations the incentives are focused on moving towards user-centric approach. The core business of the organizations and government is to provide service for citizens. It is important to make incentives transparent, so that they are applied consciously, making them more effective, and can be re-evaluated.

For example, incentives can be used to:

- Emphasize user-centricity (quality of service delivery), and/or
- Stimulate the usage of digital services by people (adoption of digital services), and/or
- Engage the government in the development and implementation of digital services (organizational transformation)

Incentives to consider

Listed below are a number of incentives that were applied in several cities and countries. They can be reused, but have to be evaluated for relevance and appropriateness, and be adjusted to the local context. Because incentives are closely related to ethics, principles and (organizational) culture, they are provided as considerations both for debate, which helps increase awareness, as well as options to implement.



Strategic building-block elements

The following incentives can be included as elements in your strategy:

NR	ELEMENT	INTENDED RESULT
1	Emphasize on user-friendliness to stimulate adoption of digital services by citizens	Digital services are designed from a user perspective and are well-supported online and offline;
2	Emphasize on speed of delivery to stimulate the adoption of digital services by citizens	Digital services promise a strongly reduced transaction time compared their non-digital equivalents;
3	Emphasize on government benefits to stimulate investing in digital service development and implementation;	New digital services are designed to decrease organizational costs and error-margins in process-chains between organizations/departments, to emphasize on the benefits of adopting them in internal business processes and the investment it may require
4	Emphasize on the reducing the number of user-interventions required to receive services;	Digital services are automated and make optimal use of available data to deliver public services;
5	Emphasize on ease of implementation of new services	Introducing new digital services is facilitated by an adaptive organization and technology;



Trust Framework

A trust framework involves a mix of technology-, legislation- and politically independent governance-frameworks, and has the aim to set the boundaries of the system; to keep it adaptive, safe and effective. Its aim is to provide an operational environment to safeguard privacy, cybersecurity, transparency and political independence.

What's the challenge?

An ecosystem of digital services relies on trust. One of the biggest challenges is to organize the control of power over the infrastructure and the transactions it facilitates. It needs to be transparent, for which technology can help. But trust needs to be built and will be gone fast, especially if related to the identity and services that influence the daily lives of citizens. This means that (cyber)security is one of the key elements to secure trust. But how do you secure digital and technology sovereignty in a time of global competition? Which checks and balances need to be in place to safeguard the public interest, and to deal with commercial or political influence?

All these challenges need an answer. Not only under normal circumstances, but also when the system is under pressure. This requires a resilient and independent framework that can cope with geopolitics, market disruptions and changes in (local) political ideology.

What's the solution?

Technology can be used to create transparency in the flow of data and give users insight into and control over their own data. To control the system, the governance framework will secure the transparency and trust. To build trust, the following basic components must be in place:

- Clear administrative structures for planning, developing and maintaining the ICT solutions. In case a country uses decentralized architecture, different (or all) ministries are responsible for their ICT developments, information systems, databased and e-services: their roles and responsibilities should be clearly established. Additionally, the state should take care of the required

structural changes in the country if needed, but in a clearly reasoned, transparent and rapid manner, so it would not affect citizens or digital developments in a negative way.

- Necessary legislation must be in place. The legislative framework must support the ICT developments in a way that the technological artifacts could be controlled, effects measured and if needed replaced. An important aspect of the legislation is that government must be politically willing to accept and endure the social and environmental changes, therefore, amend laws if processes, eco-system requires so, as long as privacy and human values are safeguarded. Government institutions should be obliged to implement various security standards by law. Technical conditions for reliable and transparent data exchange should be stipulated by law.
- Communication is a vital component and is required in planning and executing any dimension, measure or e-service. The public e-services must be needs-based, developed on the priority of existing or anticipated needs. After the development, the implementation activities must have clear messages to the target groups, and feedback from these groups must be accepted and considered in further amendments.

Cybersecurity

On a more technical level, efficient cyber security measures of the information systems will help to ensure the trust of people in the digital services provided. One of the core aims of cyber security is to ensure the uninterrupted provision of digital services and their resilience. For this, security measures should be built into the data exchange layer.



The main requirement for the information system, which links up different digital data repositories (databases), is that all outgoing data should be digitally signed and encrypted, and all incoming data must be authenticated and logged. All data requests and operations in the information system should be constantly logged, and logs chained and have non-repudiation value. These should be monitored by the related institutions, and citizens should have the power to access the portal and see which entities have access to what information. If a person wishes to examine who has access to their personal data or when that information was accessed, then she/he should receive such information from the system - thus ensuring the citizens that they have control over their data and knowledge on who has accessed it.

Trust in the digital infrastructure

The data exchange layer ideally has versatile built-in security solutions, such as authentication, multi-level authorization, high-level system for processing logs, and data traffic that is encrypted and signed. Institutions providing digital services and those hosting databases should have one or multiple security servers. Institutions with a high volume of digital requests should have multiple security servers to distribute its request load and ease the burden on a single server. The security server packages data requests in a cryptographically sound way so that the request is only accessible by the intended recipient. The security server also protects requests sent over the exchange layer from eavesdropping, unauthorized change, loss and duplication. It is the security server that enumerates possible target databases, translates register names into IP addresses, encrypts the traffic, and produces the request statistics etc.

Besides measures to prevent unauthorized access and processing of data, measures to manage cyber threats must be in place to increase trust. A country must have appropriate legislation to prevent and combat cyber threats and directly appointed government entities that are responsible for ensuring baseline cyber security and incident management. Also, the country needs legal acts

and agencies for combating cybercrime and for offering support to public organizations in case of (potential) breaches or threats.

To avoid cyber-attacks as far as possible, countries should consider working with decentralized cloud solutions which enables the possibility to switch between servers in case of an attack. This way the measurements on cyber-attacks can be solved isolated without affecting the daily operation or endanger the access to data by non-authorized organizations or individuals.

Trusted authority as independent organization

Public authority must be established or appointed as a trusted organization responsible for developing and implementing cyber security strategies and policies, coordinating the safe implementation of IT infrastructures, conducting supervision and monitoring the country's computer network and solving cyber incidents.

The trusted authority needs to be independent of the system. Meaning there is a separation of interest and function. It objectively monitors the footprint. It has the responsibility to secure a system which is effective on the long-term which means the political influence on short term is within bandwidths. With this responsibility the trusted authority always needs to be able to be transparent to the public. Meaning that not only the output of the data flows needs to be transparent but also the coding (e.g. algorithms) as well as the operation of the authority itself.

The trusted authority also needs to keep its independence of the technology; to secure technological sovereignty within the world and from technology itself. In the upcoming years the impact of new emerging technologies will put this under pressure. Within the trusted authority the responsibility of securing the human values is of utmost importance.

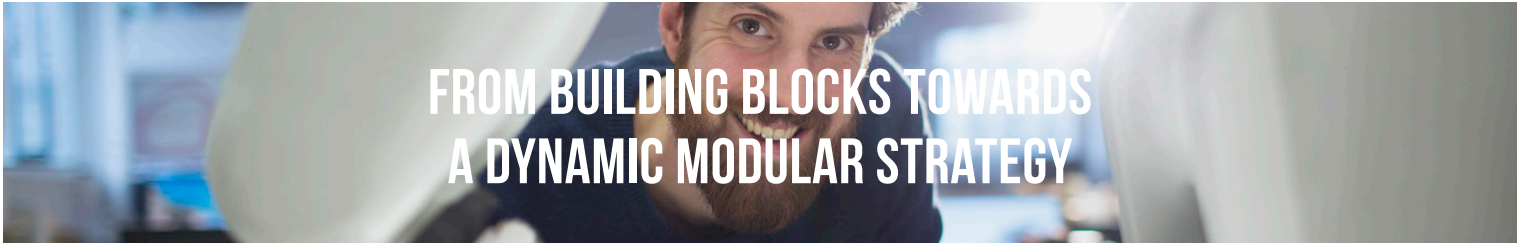
The checks and balances need to be in place (through technology, legislation and governance) that if trust is breached, measures can be taken by a country by the highest authority.



Strategic building-block elements

In order to implement your trust framework, the following elements can be include in your strategy:

NR	ELEMENT	INTENDED RESULT
1	Execute stakeholder analysis	An analysis of all relevant stakeholders, legislation and technology etc has been made to establish a clear picture of the playing field
2	Define the definition of the role, responsibilities checks and balances & escalation channels	A detailed definition of the role, responsibilities (legislation, technology, cybersecurity, privacy and communication), checks & balances and escalation channels, needed for the trusted authority to operate, is available and aligned
3	Define and decide on the positioning of the trusted authority	Based on the analysis of the playing field and the intended role and mandate of the trusted authority, the formal positioning has been decided
4	Formalize the role in the system by legislation	The independent role of the trusted authority is legally established, including mandate and rules for interventions
5	Organize the conditions for success (leadership, resources, mandate & funding)	The conditions needed for succesful independent operation of the trusted authority (leadership, resources, mandate & funding) are available
6	Implement the trusted authority on the national level	The trusted authority has been installed and is operating independently according to role and responsibilities
7	Elaborate necessary legislation for the trust framework	Legislation on all necessary aspects of the trust framework ensuring its implementation is in place to improve the system's transparency and increase public trust in the system.
9	Enforce implementation of the trust network	Monitoring, control and penalties are in place and applied when necessary, ensuring full implementation of the trust framework.
10	Embed and align technological and legal framework in Trust Framework	The legal and technical framework are designed and implemented in support of the role and responsibilities of the trusted authority



FROM BUILDING BLOCKS TOWARDS A DYNAMIC MODULAR STRATEGY

There is no single roadmap towards realizing Digital Services for Europe, or towards digital society for that matter. Every nation and municipality has its own current state of affairs. For that reason, this strategy-building toolkit isn't set up linearly, but instead provides a number of building blocks that, as a whole, cover the most important aspects of the digital and social ecosystem needed for realization of digital services for Europe, in your particular context.

Determining your starting point

To determine your starting point, this strategy-building toolkit includes a digital survey that helps identify strengths and challenges in the ecosystem of your particular municipality or country, by checking what is already in place or in progress.

For example, you might have topics already on your political agenda that have high priority, which can be used as an accelerator towards digital services for Europe? Which start-ups or existing enterprises in your environment can be used as a pillar in your strategy?

Challenges can be used as a driver for change, because priorities help to focus. Strengths on the other hand can be used for leverage, to create new opportunities and provide the confidence needed to make important decisions.

Filling out the survey is the best way to get started, because the results give an insight into your current situation. Furthermore, the process acts as a trigger to gather existing documentation and get a general overview as a country or municipality, and discuss any differences in perspective of the actual state of affairs in order to get aligned.

Creating your local roadmap

Although each of the building blocks is different in nature and seems to stand by itself, there are natural links between them that can be brought into alignment in such a way that a "route" emerges.

For example, strong digital leadership is a great asset to create awareness and to implement digital principles. Having principles in place is of importance to effectively procure and/or develop a technological infrastructure. This in turn provides a basis for the actual digital services, and so forth. In this manner, a logical chain of events comes in place that provides a possible course of action.

Another starting point could be the existence of a strong ecosystem of startups or tech-companies in your region that can be employed or partnered with to develop services, organize support or host services. Using a regional strength such as this can help to create a regional identity. This in turn facilitates the positioning of digital leadership and appoint a strong digital leader.

The Dynamic Roadmap Tool allows EU-municipalities and Member States to generate a strategic roadmap to create an ecosystem for developing, implementing and delivering human-centric digital services.

Visit <https://www.digitalservicesfor.eu> and get started on your local strategy!



The appendices presented below, consist of a number of specific use cases from several European countries and municipalities that have taken steps to implement digital services in their context. These use cases have helped lay the foundation for the strategy presented in this document.

The sections below provide a more in-depth description on a number of solutions that have been put into practice, as well as more detailed information on several of the elements discussed in the strategy.



**APPENDIX:
BACKGROUND OF LEADERSHIP BUILDING BLOCK**

Digital Transition is the process of adaptation that comes along with the technological, cultural and social phenomenon that is called the Digital Revolution. This transition eventually impacts all processes, workflows and the perspective on the way we work together. Such profound changes will be received with reluctance, sometimes even rejection and resistance. It is obvious that such far-reaching shifts cannot be implemented successfully without the proper leadership.

Thus, the digital transition of an organization can only be achieved in combination with capable leaders. Digital transition leaves nobody in the organization untouched and on top of it all it happens at a high pace, meaning leaders need to quickly anticipate changes and know how to deal with them. They also need to address reactions from the workforce. Leading a digital transition means not only understanding the technological aspects but also the social implications. Being a successful digital leader means understanding that it is a people's business. Therefore, first of all a digital leader needs to be installed and he or she must be equipped with the appropriate skills.

But communication does not stop at the top level nor does it phase out over time. One cannot simply assume that the information about the necessity for organizational change will trickle down to the various levels of the organization, especially since cultural persistence has been identified as one of the most challenging aspect in the transition process. Public servants of all levels need to be addressed, involved and made aware of the necessity to change the approach how to serve citizens – time and again.

Communication is at the core of it all, and we therefore recommend as a first step in the whole process the creation of a position along the lines of Chief Digital(ization) Officer (CDO), who reports directly to the mayor, who has the mandate to instigate that change and who is responsible for promoting that shift. If you do not have your leadership in place, you won't be able to relate your vision. If you do not commit yourself to that task, the CDO will fail.

This leads to the content that actually shall be communicated. One has to imagine how a rather

immovable organization as the public administration, that does not follow business models and revenues like private companies, typically is, can be made ready for that change. It must be assumed that so far there is no knowledge on the necessity, the benefits and impacts of modern technology on the business models.

A vision of how a modern public service can address the citizens' needs therefore to be elaborated. Where does the organization want to be in a certain period of time, how does it want to do its job, how does it want to satisfy the citizens' demands and how does it want to structure, develop and implement its service procedures, all of that with the implementation of modern technologies.

A digital leader must offer a vision for the future. Devising a clear and coherent digital strategy is the first step toward successful digital transformation. The attributes of a digital-age organization—agency-wide governance focused on the customer, processes that tap into the potential of data, and a passionate and aspirational workforce—must be articulated and such a vision must be clearly communicated to the workforce.

From the vision derives the strategy, and the importance of a clear strategy is undeniable. Government organizations can benefit from a roadmap that addresses the key elements of digital transformation: culture, leadership, workforce, and procurement. But the strategy must be accompanied by a mechanism to track and measure progress against the digital goals. It needs to be stressed that culture is one of the most challenging aspects in transition. The digital leader needs not be swayed away by the organization's institutional inertia. Positive results will speak for themselves and remove opposition.

Cultural change is complex and exhausting. The CDO needs to determine what needs to be changed. He/she needs to ensure strong support from the top level, and make clear to all departments the need for change. He/she needs to understand the doubts and concerns of the organization, which means one needs to identify the processes, legislation, and cultural elements that could hinder digital transformation, and devise strategies to move past each of these barriers. Once the organization is willing to move, the CDO needs to communicate often, be transparent and dispel rumours. He/she needs to involve people in the process. Once the desired change has been achieved, the CDO must make sure that the results are



incorporated into the organizational culture. Naturally, any switch to the old format must be avoided by means of developing ways to sustain the change. That also includes support and training where needed. In order to dispel concerns it is also extremely helpful to point to success stories.

Provide a detailed plan for addressing the key elements of digital transformation. Build a roadmap for digital transformation that covers elements such as culture, leadership, workforce, and procurement. For instance, detail how to engage stakeholders and secure their backing to implement the strategy or describe how procurement processes could be reformed for the digital delivery of services.

Digital leadership

Digitization must be a top-level priority. It is a cultural change that transforms all processes in the organization, therefore it is of utmost importance to include all levels of hierarchy, beginning at the very top.

A central strategy is important, although this is not always easily achievable. If departmental leaders still cling to the past, changes for the future will not be possible.

Nonetheless, people's approach towards digital services is changing fundamentally and certainly not a zeitgeist phenomenon. The structural changes that come along with the digital revolution are perpetual and need to be regarded as such. Digital transformation is not like a common cold that comes suddenly and goes away shortly after.

Therefore, all the highest hierarchical levels need to be involved and need to commit themselves to supporting all measures that address these changes. The organization as a whole, needs to embrace the transformational process and understand what comes along with it.



APPENDIX: BACKGROUND OF PRINCIPLES BUILDING

The Ministerial Declaration on eGovernment

The Ministerial Declaration on eGovernment, regularly referred to as the Tallinn Declaration was signed by all the European Union Member States and EFTA countries in Tallinn on 6 October 2017.

This marks a new political commitment at EU level on significant priorities towards ensuring high quality, user-centric digital public services for citizens and seamless cross-border public services for businesses.

The Member States reaffirmed their commitment to progress in linking up their public eServices and implement the eIDAS regulation and the once-only principle in order to provide efficient and secure digital public services that will make citizens and businesses lives easier.

The Tallinn Declaration provides an important impetus for Member States and the Commission, both collectively and individually, to continue to invest in accelerating the modernisation of the public sector.

In the annex of the Declaration, Ministers in charge of policy and coordination of digital public services in the countries recognise the needs and expectations of citizens and businesses as they interact with public administrations. They commit to designing and delivering their services, guided by the principles of user-centricity (such as digital interaction, reduction of the administrative burden, digital delivery of public services, citizens engagement, redress and complaint mechanisms).

For the principles of digital-by-default, inclusiveness and accessibility, we will:

- ensure that European citizens and businesses may interact digitally with public administration, if they choose to do so and whenever feasible and appropriate from a cost benefit and user-centricity perspective;
- work to ensure the consistent quality of user experience in digital public services as set out in the Annex “User-centricity principles for design and delivery of digital public services” of this declaration;
- work to increase the readiness of European citizens and businesses to interact digitally with the public administrations;

For the principle of once only, we will work to implement it for key public services, at least as an option for citizens and businesses;

For the principle of trustworthiness and security, we will:

- ensure that information security and privacy needs are taken into consideration when designing public services and public administration information and communication technology (ICT) solutions, following a risk-based approach and using state-of-the-art solutions;
- work to increase the uptake of national eID schemes, including to make them more user friendly and especially more suitable for mobile platforms, while ensuring their appropriate security levels;

For the principle of openness and transparency, we will make it possible for citizens and businesses to better manage (e.g. access, check and inquire about the use of, submit corrections to, authorize (re)use of) their personal data held by public administrations, at least in base registries and/or similar databases where feasible;

For the principle of interoperability by default, we will work on national interoperability frameworks based on the European Interoperability Framework (EIF), while respecting also the relevant national standards, and adhere to EIF for cross-border digital public services.



APPENDIX: BACKGROUND OF LEGISLATION BUILDING BLOCK

Legislation-toolkit for nations

Digital signatures act

The main aim of the act is to equalize digital signature with paper-based signature, i.e. give digital and handwritten signatures an equivalent legal status. The act clearly stipulates that digital signature has the same legal consequences as a handwritten signature. As a rule, digital and handwritten signatures must be equivalent in document management in both public and private sectors.

The legal act sets forth the requirements that digital signature must uniquely identify the signatory, enable determination of the time when the signature is given, and be bound to the signed data in such a way that makes changing the data after signing impossible without invalidating the signature.

Crucial for the transition to digital governance, this legal act should oblige all public institutions to accept digitally signed documents. As of 2016, this is required also by eIDAS Regulation at EU level (date of enforcement: September 2018).

Public information act

Beside Digital Signature Act, this is one of the cornerstone legislation on digital governance, laying ground to the entire national information system and ensuring public access to it.

First, the act obliges the public entities to make information available digitally and grant public access to it. The act also obligates public entities to maintain websites and post relevant information online. These entities are also required to ensure the relevance and clarity of the information.

The public and every person has the opportunity to access information intended for public use and to create opportunities for the public to monitor the performance of public duties. People have the right to make inquiries, and the act obliges the holders of relevant information to reply to any request.

Second, the act stipulates the establishment of the government digital portal(s) via which public digital services are provided, including the roles and responsibilities for maintaining and development of the portal. Similarly, obligation(s) to organise the portal in user-centric manner is stipulated in the act.

Third, the act regulates the establishment and management of public databases (data repositories), including roles and responsibilities, and access to these databases. The databases must be digital and connected to the state information system. The act prohibits the establishment of separate databases for the collection of the same data, i.e. enforces once-only principle to be followed in practice.

Forth, the act provides a legal ground for the data exchange layer within the state information system. The act stipulates that the exchange of data with the databases belonging to the state information system and between the databases belonging to the state information system shall be carried out through the data exchange layer of the state information system.

Besides the above, the act also obliges public entities to manage digital document registers (for incoming and outgoing correspondence), regulates restrictions to the information system and outlines supervision duties.

The act covers national and local government agencies, and other legal entities both in public and private law that are responsible for the delivery of public services in areas such as education, health care, social or other public services.

Personal data protection act

As of 25 May 2018, the directly applicable EU Regulation (General Data Protection Regulation) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data began to regulate the personal data protection law.

Member States have been given discretionary power in certain issues to specify, establish and preserve the issues relating to personal data processing provided for in the general Regulation, thus the right to elaborate on and supplement the GDPR.

The topics may include f.e. protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution



of criminal penalties, and on the free movement of such data. Another example might be establishing in conformity with GDPR a few exceptions to the general principle of the processing of personal data, f.e. in the processing thereof for journalistic purposes as well as for the purpose of scientific and historical research.

The act may also foresee applicable fines in case of violation of personal data protection regulation.



APPENDIX: BACKGROUND OF TECHNOLOGY BUILDING BLOCK

Digital identity

To achieve a single digital government, a digital identity is required for all residents of your city/country. By enabling identity in a safe and easy way, citizens are enabled to do business themselves easily with the government and the business community, in which they can control their data.

The disclosure of the digital identity must be fast, easy and accessible to citizens and companies in which all key registrations of local and national government are made accessible. In addition, the identity must comply with GDPR, eIDAS, PDS2 so that it is compliant with European legislation.

Next to the identity of people there also needs to be a registration of objects & organizations. People interact within a context (e.g. subway, stadium, company). With the rise of IoT and sensing (accelerated by 5G) the identity of the object becomes the core for data protection. In the upcoming years the dependency of these objects on a daily basis will increase. The value that will be generated through this will increase by a fiftyfold of the current data market. The value and usage that is generated by the object will go back to the user. By creating a unique identifier for objects people, technology and organizations are able to interact with each other.

In order to make it work there are a few elements which need to be implemented:

- A core identity which is accessible for governments and business (responsibility National government)
- Safe and secure register for people, objects and organization. (responsibility National government)
- Identification and authentication layer whereby citizens/customer & organizations sign up, log in, sign a digital transaction or digital document and identify themselves. (market but approved by government).

Data exchange layer

The data exchange layer is the technology that enables the citizen to get control over their data. It makes it

possible to achieve secure data exchange via the internet. As a result, local and national databases can be made accessible in a simple and standardized manner, allowing parties (government and business) to easily and quickly offer digital services to residents and companies in which the overview and control lies with the resident and the responsibility with the service providers. The technology guarantees transparency because the data exchange is automatically tested against the authentication and authorization standards.

Currently most organizations are built up out of silos. This is translated into the application landscape which is fragmented, processes, applications and data are organized next to each other. Working together with other organizations makes it difficult of even impossible to work in a customer driven approach.

By implementing a decentralized and independent data exchange layer in which service providers can connect quickly and easily, we ensure that the data and applications are separated. This enables the once-only principle and to gives back the control of data to the end users (residents and companies).

So what do you need to do? In order to make it work there are a few elements which need to be implemented:

- An independent data integration layer that is capable of authentication, "multilevel" authorization,
- A high-quality logging system and encrypted data management including time logging.
- Central security server; access portal for service providers that guarantees that all connected information systems meet the (technical and security) standards of the data integration layer, services and roles, data traffic (encrypted) and audit trail are guaranteed (evidence) (incl. central and local monitoring system)
- Proxy configuration; development environment to further develop the data exchange layer and security server.

Sensing and service

Services

Services (government and business) are based on 6 simple steps (need, solution, order, delivery, payment & follow-up). These 6 steps do not differ from the type of services



that goes through; not between services & products, not between market & government. This gives focus because if this is in place you can start working on your digital services. The big advantage is that these steps are already in place. The technology is there. By implementing these microservices through API's your system can interact. There are two important requirements to secure; the API boundaries to enable interoperability (and avoid vendor lock-ins) and the data platform they use; it needs to be independent based on "docker technology" (to avoid platform lock-in). The last point is very important from a legislation perspective as well. The data can't "leak" away (f.e. for a US platform like Amazon is different legislation in place which makes it difficult to become GDPR compliant).

Sensing

A new dimension is sensing. The number of sensors and cameras in society is increasing in rapid pace. Everything is getting connected which enables the machine to machine revolution (which will decrease human transaction dramatically). The overview of the sensors will be of big importance to enable the possibilities to interact with the services (humans & technology) and safeguard the public interest by using the data exchange layer.

So what do you need to do?

In order to make it work there are a few elements which need to be implemented:

- Implement the microservices & Sensing/IoT into a platform which is curated by the government (or independent authority). This way the API strategy & data protection is secure, and you enable the market to innovate and develop.
- Develop or stimulate (through marketing) an implementation strategy for cities and businesses to implement the products & services

Interface

Why do you need the interface?

The interface layer is the key to successful implementation of digital services; this is what citizens, businesses and back-office officers experience and which will increase trust (if done properly). But only the front is insufficient;

the backend must be as simple as possible, with maximum machine to machine interaction. The interface layer needs to be based on microservices to secure modular adaptive technology. At this moment the interface layer is visible through websites and apps. In the near future the upgrade towards Augmented Reality (AR) and Virtual Reality (VR) will be there. By using modular technology digital services can easily be upgraded without big investments (in time and money). This way organizations become adaptive in upgrading services.

What problem does it solve?

At this moment the interface layers, to deliver services towards citizens, of government and businesses are fragmented and based on the product push of the organization. It is not human centered. This creates an overkill in which people get lost. Instead of the need of the citizen/customer, the product of the system is leading. The backend of the interactions (executed mostly by back-office employees/civil servants) are often not aligned with the frontend solutions (due to vendor lock-ins). The impact is bad services, longer waiting and more handling costs & time. Because of this most government and businesses are not able to upgrade their services and do not make use of the insights of the data which helps them to improve the quality of services. This way organizations are stuck in developing fast and simple solutions with the latest technology.

But the solutions are there. Especially within big tech companies this problem is solved through simple modular interface layers based on microservices. The technology is there. The challenge is to implement it.

What is the solution?

By developing the interface layer via a modular platform based on microservices & business engines, we are able to deliver standardized customization, enabling the organizations (government and business) to deliver more effective and efficient services to citizens and customers. The platform enables the possibility to let business developers built their own services without coding, get direct insight in the operation and needs through dashboarding and manage their operation with machine-to-machine technology. This helps organizations to become adaptive and break free from the current legacy.

14] Background information on container technology



Within the interface layer there are two interfaces; organization & customer view. Underneath both views are explained:

- Customer view; an interface layer in the form of a web application (applicable for all devices) with components which are easily upgrade to Augmented reality layers. The interface enables citizens to keep control over their data and through customer journey businesses and government offer services through customer journeys.
- Organization view is defined in four different elements:
 - Operational layer; the services are as much machine-to-machine as possible. But to manage the operation of the organization it gives the overview of the actions the back-office (might) need to take and enables communication for second line communication with customers (first line is solved through chatbots).
 - Dashboard (including AI & cybersecurity); the organization gets overview through the dashboard in the steering of its organization (the volumes, production, communication flow (happy flow and exceptions). It also shows the authorizations and usage & flow of the data to secure the usage and to recognize patterns to adjust & develop services.
 - Customer journey manager; the no-coding principle is enabled by the customer journey manager which makes it possible for policymakers, business developers and/or manager to design, test and implement their services.
 - Object layer; through the sensing platform and the exchange layer the information of the sensors extracted and gives insight and overview of the data of cities. The object layer gives insight and enables cities to manage their information flows in an easy way. This layer is able to visualize different layers of the city and enables cities to move forward into a digital twin. In the near future the customer view will upgrade towards AR and VR which makes it possible to interact real-time with the object layer.

In order to implement the different views cities do not have to develop the views themselves. Most building blocks are already in place and operational. The challenge is to build the interface platform and scout the right microservices which are compliant. On a view building the blocks the market might be challenged (if they are not already doing this). The role for cities is to govern and curate the platform and help implementing it on National or local level (depending on the choice a city/country makes in their strategy).

What do you need to do?

In order to make it work there are a few elements which need to be implemented:

1. Decide as country and cities who is responsible for the interface platform for digital services;
2. Organize the multilayered governance to enable the conditions;
3. Define the independent procurement organization to develop the platform (by using existing technology and building blocks) to secure the knowledge;
4. Develop the platform based on a multiyear roadmap (including an emerging tech roadmap on technology);
5. Organize the implementation team or partner to execute and implement the interface layers with cities.

Digital data repositories

How do you get from a system of national registrations, sector registrations and local registrations to a uniform data landscape that meets the life event needs of citizens and entrepreneurs? The (re) use of data offers many opportunities. How do you secure that citizens are able to view, share and (re) use data by having direct access to their data sets as available in the various basic registrations, sector registrations and local registrations?

In order to deliver seamless digital services to citizens and to secure the once only principle the data repositories need to be available for all government & business data. The first important step is the establishment of the core registrations in which governments can access each other's basic data and is enabled (via the data exchange layer) towards citizens and businesses (in a secure way). This leads to a fundamental improvement in efficiency and effectiveness of the government services and to connect business.

Modernization of the service calls for broader sharing of data. This requires the release of data from the silos. The data is decentralized but the control principle is human centered which means the insight and control is with the end user. This creates a level playing which makes interoperability between the government and business possible are and residents and entrepreneurs themselves control their data.

In order to achieve a more uniform way of the re-use of information, citizens and entrepreneurs must be given the opportunity to have direct access to the core registrations of the government. Changes to these registrations are



implemented directly throughout the entire chain. Real time and without intervention from third parties; machine to machine.

The cloud

Cybersecurity in this development is a big concern. To ensure that the data is secure and resilient for cyber-attacks it's important to bring the data to the cloud on several servers. You need a decentralizes network of servers to ensure you are adaptive in case of a cyber security attack to switch between servers and secure that the end user won't any difference. Not only because the daily life of citizens and businesses depend on it, but equally important, to keep the trust in government. The process of building trust in digital services takes time. To keep this trust the citizens and business need to be able to rely on the basic infrastructure.

Within this transformation it's important to create a migration strategy to bring the data to the cloud. Set by set. This migration towards the cloud should start with the data repositories on National level. This is the most effective and secure way because it's easy to manage and through the data exchange layer local governments and business can directly start using this data and start building new services. This way local repositories will become obsolete. Which saves time, energy and is more cost effective. By building this as plug and play the trust, and more important usage, will start from the first moment.

The following data repositories need be standardized to secure your data strategy:

TYPE OF DATA SOURCE	LEVEL
Population register of persons (consists of residents and non-residents)	National
Commercial & Trade Register	National
Registration Addresses and Buildings	National
Registration Topography	National
Land register	National
Land board geoportal	National
Immovable portal (vehicle Registration)	National
Registration Income	National
Building register	National
Registration Value Real Estate	National
Registration Large-scale Topography (formerly GBKN)	National
Registration Subsurface	National
Sensor database	National/Local
Education information system	National

When the data strategy is realized the following results will be delivered:

- Governments develop services that are directly linked to basic registrations and users (citizens and entrepreneurs)
- Governmental data from the core registration are available and accessible safeguarding privacy & security based on European standards. The data is findable, available and usable, within and outside the government, where the user is responsible for proper use.
- To secure the footprint, the data transparent about the data use process. This way accountability, privacy and freedom of choice is guaranteed
- (Re) used data is reliable and up-to-date
- Various data sets from basic registrations can be linked with the aim of better services and / or enforcement

So what do you need to do?

In order you need to be successful the following steps need to be taken:

1. Analyse the core data repositories based on the white label and define who is responsible and accountable
2. Organize leadership (responsibility) and execution (accountability) on the data strategy
3. Develop the data strategy for the data depositories (centralized/decentralized & cloud).
4. Analyse the separate databases on data quality and technical requirements to define the current situation
5. Develop the migration strategy to phase in the core data repositories
6. Implementation per data repository based on migration strategy
7. Fading out of local and decentralized data repositories (monetization strategy)

Certification center

The structure of the government strategy is based on principles, legislation and technology. Based on the principles in the Tallinn declaration on eGovernment on openness, interoperability and transparency the key is to secure trust. It's principle-based instead of rule-based. To secure the footprint with a technical instrument these principles are secured. This role needs to be executed by an independent party, apart from politics and business. Depending on the layer, governance is organized in which the communities (based on knowledge) play a validating role



In order to support the system (principles, legislation and technology) the organization that guarantees the reliability, transparency and agility of system control. This organization has an independent role that guarantees separation of functions, allowing it to act independently.

What is the solution?

To support the organization there needs to be a certification center which is a technology that has several functionalities:

1. Entrance and monitoring of organizations (purpose, roles and services)
2. Independent monitoring on the execution of the system; it visualizes the movement within the data which automatically shows the patterns on roles, authorizations and services (based on the principles and legislation). It triggers messages on misbehavior, breach of privacy, cybersecurity risks and patterns to improve services based on needs.

So what do you need to do?

1. Functional design and testing of the certification center with business rules (including purpose of the organization, roles and services) and the data monitoring including pattern recognition. (not the content of the data)
2. Technical implement the certification center
3. Organizational implementation of the certification center within the Trusted Authority



APPENDIX: BACKGROUND OF TRUST FRAMEWORK BUILDING BLOCK

Access logs

Standardization of access logs is important to make it easier to log requests. All data request templates in the information system should be prefabricated and no free-form requests like “find all black cats on the White Street” allowed. A logged request might look like this: On the 15th Day of September 2015, precisely at 13:47:12 and 85 microseconds, the Person numbered as 37412029381 on behalf of the Business Register Entity no. 12345678 made a “Find-The-Owner-Of-The_pet.wsdl” (WSDL) request against the “Pet Register”.

Trusted authority

Public authority must be established or appointed which is responsible for developing and implementing cyber security strategies and policies, coordinating the safe implementation of IT infrastructures, conducting supervision and monitoring the country’s computer network and solving cyber incidents.

Estonia - institutions

MKM is responsible for the overall development of public services, standardisation, the establishment of a user-friendly service environment, electronic communication, cyber security and increasing citizen’s awareness about the opportunities and threats existing while using the Internet.

The Estonian Information System Authority (from now on RIA) coordinates the development and administration of the national information system, such as X-road, eID, RIHA, eesti.ee and CERT (RIA, 1.05.2016), the listed components will be viewed in greater details under the technology paragraph. However, it is important to note RIHA’s function.

RIHA is an administration system for the state information system which means that it has two primary purposes. First is to serve as a catalogue of the 21

state information system, databases, information collected, services connected to x-road lists the reusable components. And secondly, RIHA records the use of information systems and databases, register services, connectivity with x-road and administer the reusable components such as XML assets, classifications, dictionaries and ontologies.

RIHA is a catalogue for the state’s information system and a procedural and administrative environment

The Centre of Registers and Information Systems (from now on RIK) develops and administrates many information systems. The list is following: the e-Business Register, the e-Notary system, the e-Land Register, the information system of courts, the Probation Supervision Register, the Prisoners Register, the Criminal Records Database, the e-File, the electronic State Gazette, etc. (RIK, 24.04.2016). The Information Technology Centre of the Ministry of the Environment (from now on KEMIT) administrates and develops information and communication systems of the Ministry of the Environment (KEMIT, 24.04.2016). The Information Technology Centre of the Ministry of the Finance (from now on RMIT) administrates and develops Information and communication systems of the Ministry of the Finance (RMIT, 1.05.2016). The Information Technology Centre of the Ministry of the Interior (from now on SMIT) administrates and develops information and communication systems of the Ministry of the Interior (SMIT, 1.05.2016).

As the architecture of Estonian Information System is decentralized all the ministries administrate the development and management of their internal information systems which must be by the Estonian Interoperability Framework (MKM, 1.05.2016). information systems which must be by the Estonian Interoperability Framework (MKM, 1.05.2016).



APPENDIX: BACKGROUND OF PROCUREMENT BUILDING BLOCK

Engine, microservices & container strategy

The procurement strategy provided below targets mainly the implementation of a micro-service architecture, due to the increased importance of agility and scalability. As this type of architecture is quite a leap from the current silo-based software solutions that are in place, a(n interim) service-based architecture could be considered as part of a transition plan. However, especially where greenfield options are available, micro-service architecture should be given preference whenever possible.

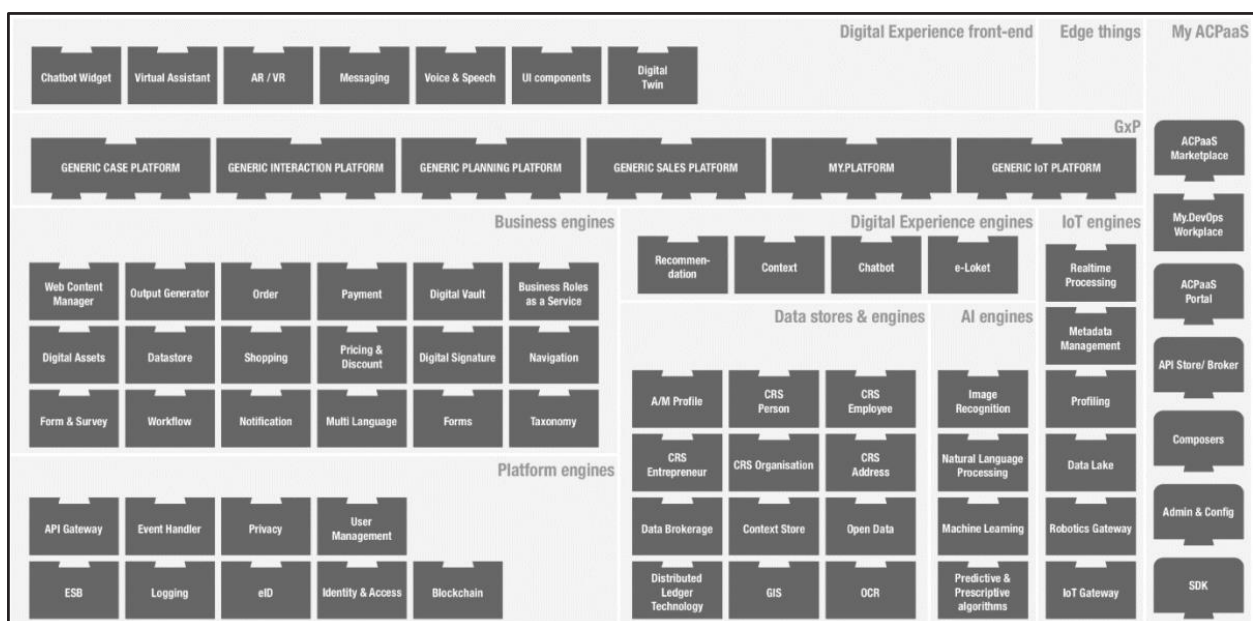
To get the agnostic technology in place, the digital components and functions of the platform need to be described. Based on the example of Digipolis (service provider for the city of Antwerp in digitalization) there is a definition of the core components divided in three categories:

1. Microservices; a microservice is not a layer within a monolithic application (example, the web controller, or the backend-for-frontend). Rather it is a self-contained piece of business functionality with clear interfaces, and may, through its own internal components, implement part of a layered architecture.
2. Engines; an engine is a generic software component

that enables the microservices to work and generates the right datasets. The engines can be developed separately but need to be coherent to secure interoperability. The engines are divided in different components with different functionalities. These components can be clustered in the type of functionality that they offer (e.g. core engines, IoT engines, Digital Experience Engines, Intelligence Engines, Engine clusters).

3. Container technology; Platform-as-a-Service (PaaS) or platform-based services is a category of cloud computing services that provides a platform allowing cities to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. The platform which uses OS-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries and configuration files; they can communicate with each other through well-defined channels, some only within the government, while other may also be available to third parties. All containers are run by a single operating-system kernel and are thus more lightweight than virtual machines. Another advantage of container technology is portability, scalability and zero-downtime deployment.

The technology building blocks are translated into a framework which is visualized underneath based on the core components of Digipolis' ACPaaS:





The core is the basis for the procurement strategy. The advantage of this approach is that several components are already available and can easily be applied. If there are components which are not available, they can be added through procurement. Within the platform there is no exclusive right for providing a particular solution, most important is that elements fit within the framework and are compliant with legislation on European level. This means that for some microservices or engines there will be several solutions available simultaneously that cities can choose from (e.g. payment services are microservices of which several are already available).

The strategy is based on an adaptive procurement framework, which means that within the platform, due to new technologies, it is simple to add microservices and engines. This enables a faster procedure of procurement and stimulates innovative companies or start-ups to anticipate.

COLOPHON

Copyright © 2020 Urban Agenda for the EU,
Digital Transition Partnership

Authors:

Hillen Oost

Jonas Onland

Kadri Jushkin

Patrick Schwind

Tomislav Uroić