SUSTAINABLE DEVELOPMENT GOALS

Introduction to e-Government

e-Government to Support Sustainable Development Goals

eGA e-governance academy
15 YEARS Empowering e-governance around the world

Introduction to e-Government

e-Government to Support Sustainable Development Goals

eGA e-governance academy
15 YEARS
Empowering e-governance around the world

Author:
Hannes Astok

Contributors:
Arvo Ott
Uuno Vallner
Niall McCann
Katrin Nyman-Metcalf
Olav Harjo
Raul Rikk
Kristina Reinsalu
Aleyda Ferreyra

Photos:
e-Governance Academy, Schutterstock, estonia.ee

Design:
Gerit Tiirik (Sviiter Creative Agency)
www.sviiter.com

Published by:
e-Governance Academy
Rotermanni 8, 10111 Tallinn, Estonia
ega.ee

The e-Governance Academy is a think tank and consultancy organisation founded in 2002 for transfer Estonian and international experience in the areas of e-government, e-democracy, and national cyber security. In its 15 years of existence, academy has assisted e-government development in more than 60 countries by making their decision-making processes more transparent, democratic, and less encumbered by bureaucracy.

This text was developed as part of Hannes Astok internship in UNDP Headquarters in 2017.

This publication is composed by support of

ESTONIA
DEVELOPMENT COOPERATION

PERMANENT MISSION
OF ESTONIA TO THE UN

ISBN 978-9949-81-985-0

This publication will help you understand the **elements and key challenges** of e-government. It will not go deep into technical issues nor provide guidance on setting up an e-government within a government.
The text is based on the experiences of its contributors, who have participated in e-government projects around the world. It is meant **for professionals of all levels** dealing with governance projects.

Hannes Astok
Deputy Director of
e-Governance Academy

Contents

Information society, individuals and governments

Information society is a comprehensive concept. It impacts individuals, organizations and governments. Information and communication technology (ICT) has changed and is continuing to change remarkably in today's world. And we are not even aware of all the upcoming changes.

Information society redefines the notion of geographic location. It decreases distances both within and among countries and removes borders. It also helps regions develop and become more competitive.

The development of information society affects the nature of human activities in many ways. It allows us to work remotely and more efficiently, communicate easily and cheaply over long distances and eliminate labor-intensive jobs. By introducing digital technologies into the work processes of government, information society creates transparency and new opportunities for enhancing democracy and fighting corruption. New technologies enable better access to finances via virtual banking solutions and can help local businesses go national and regional businesses go global. It is all possible because access to information is easier than ever before in human history.

The tools of information society, properly implemented, can provide better access to health care, education and social services for billions of people.

Developing information society is one of the key elements of the United Nations' Sustainable Development Goals (SDG) for coping with global problems. It is not a silver bullet that will solve all problems automatically. Only dedicated and consistent action by governments in cooperation with civil society and the business sector can bring about the possible changes and improvements.

Because of the global importance of ICT and the future changes it will cause, many governments have taken a leading role in the development of information society. Indeed the roles they play are crucial, not only as facilitators and leaders, but also as enablers and regulators. The power and resources of government are limited, however, making the involvement of all stakeholders, in transparent cooperation, the key to success.

The main areas of government involvement are the following:

- Passing new legislation
- Supporting development of the private sector
- Improving interactions between government and citizens
- Raising awareness of information-society challenges and opportunities
- Developing human capital
- Modernizing public administration
- Building e-governance infrastructures

Goals to achieve

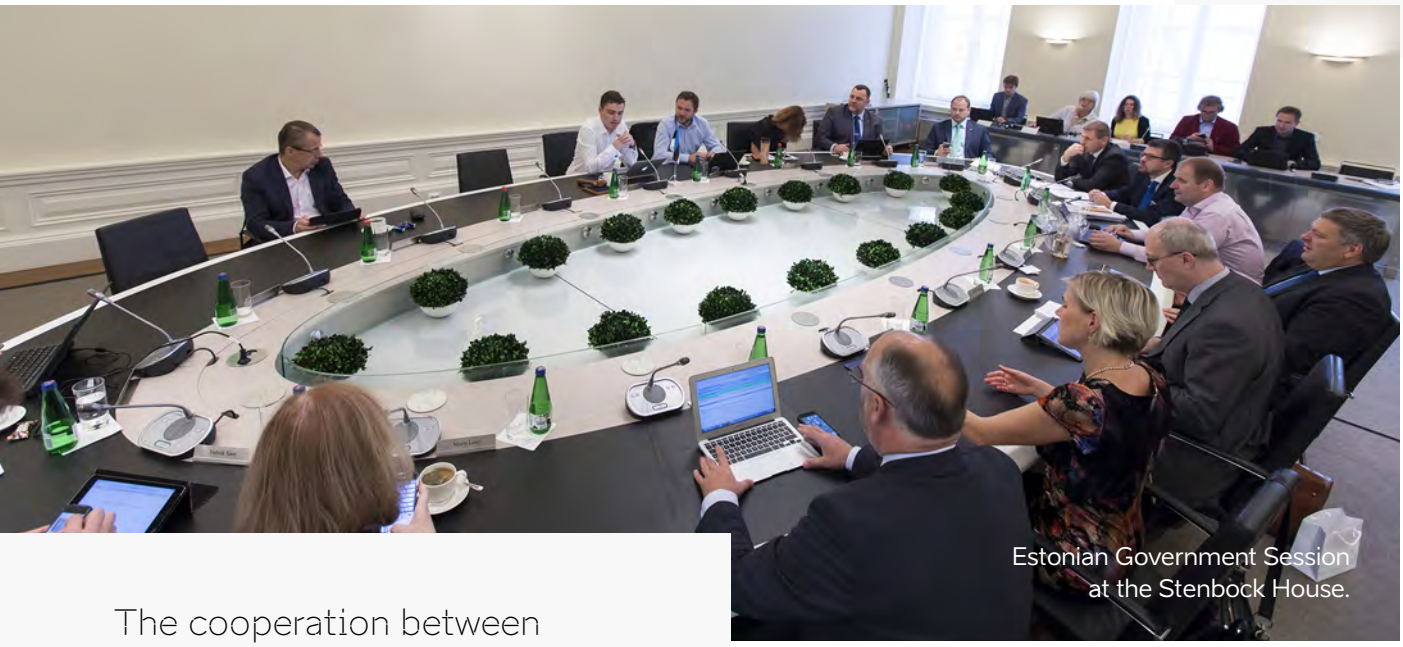
The policy for the development of information society is usually called information policy. The goal of information policy and related action plans is to form a society in which government serves its citizens, promotes their participation and cares about their wellbeing.

The goals of information policy are to:

- Promote and ensure democratic and inclusive processes
- Support the development of an information infrastructure
- Support the formation of a competitive economy, including transforming the traditional economy and building a digital economy
- Support the development of citizens' digital skills and related education
- Support the development of culture and local languages, respecting the value of cultural diversity
- Support the modernization and improvement of government processes

Information policy should foster the creation of a sustainable social and economic environment that, in turn, can support the creation of new forms of entrepreneurship and civil society. It should serve to decrease bureaucratic barriers and prevent "information haves" and "information have-nots" from appearing as social groups or as regions. The ultimate goal of information policy is to increase prosperity and welfare in society.

E-government development



Estonian Government Session at the Stenbock House.

The cooperation between government and the public sector, referred to as Public Administration, comprises the most integral part of information society. This is what we mean when we use the term e-government.

People think that e-government is only about technology and the computerization of government. Not so. To make a real impact on society, to achieve efficiency in government and to reach the goals of transparency and accountability in all government processes, e-government takes a much broader approach.

By definition, e-government entails a comprehensive set of organizational, regulatory and technology-related measures. To receive the full benefit of digital technologies — computers, tablets, servers, telecommunication networks, data and document exchange solutions, smart ID cards — governments must be ready to change their processes and put in place necessary regulations.

If these measures are not taken, digital data and transactions will be deprived of their function and meaning: data is not re-used, service delivery processes are copied from the paper era with no changes, computers are used as typewriters, application forms are printed out in government offices and all incoming information is manually re-submitted back to databases.

The problem with most e-government projects is that they focus too much on technology implementation. Usually what is lacking is focus on organizational setup, business processes and regulatory development. In the end, the technology is functional and in place, but it is not integrated into government processes in a sustainable way and with proper institutional and legislative support. Supportive services are often not implemented. As a result, more time is required to convince government departments and their legal offices to use

> The problem with most e-government projects is that they focus too much on technology implementation.

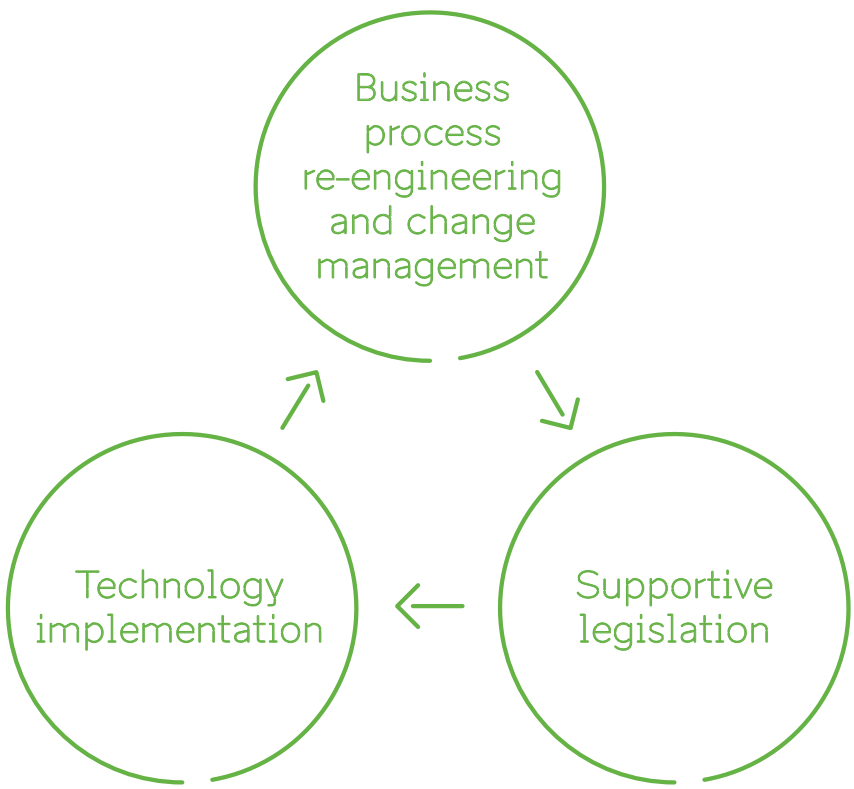
the technology. And sustainable financing goes missing after implementation, which is often financed by a single source.

Political leaders must support all the necessary processes to bring about real change. Their counterparts in ICT departments may be educated, enlightened and enthusiastic, but they cannot reduce government bureaucracy and working habits by themselves.

High-level coordination of e-government activities among the various departments of government is also crucial. The ideas, projects and programs of a given country must fit its framework. Standards, policies, legislation and regulations should be developed to make available nationwide data re-use, data exchange and digital identity. Investments in ICT infrastructure and solutions must be monitored to avoid duplication and over-investment. And appropriate draft legislation must be prepared for government ministers and members of the government's ruling bodies.

High-level coordination does not envisage an entity that handles all ICT questions and procures new computer keyboards when the old ones are stained with coffee. To the contrary, all ministries must be able to run themselves. They must be enthusiastic about modernizing their business processes and innovating new services, while ensuring that data, infrastructure and online services subscribe to common frameworks.

Technology implementation is thus sometimes the easiest part of the process.



Key elements of e-government

We can divide the key elements of e-government into two sections. One section is **"digital elements"** and is directly connected to technology. The other section is **"analog elements"** and supports the technology with regulations, organization, financing, change management, raising awareness and political will. These sections are not opposed to one another but rather complement each other.

Key digital elements of e-government

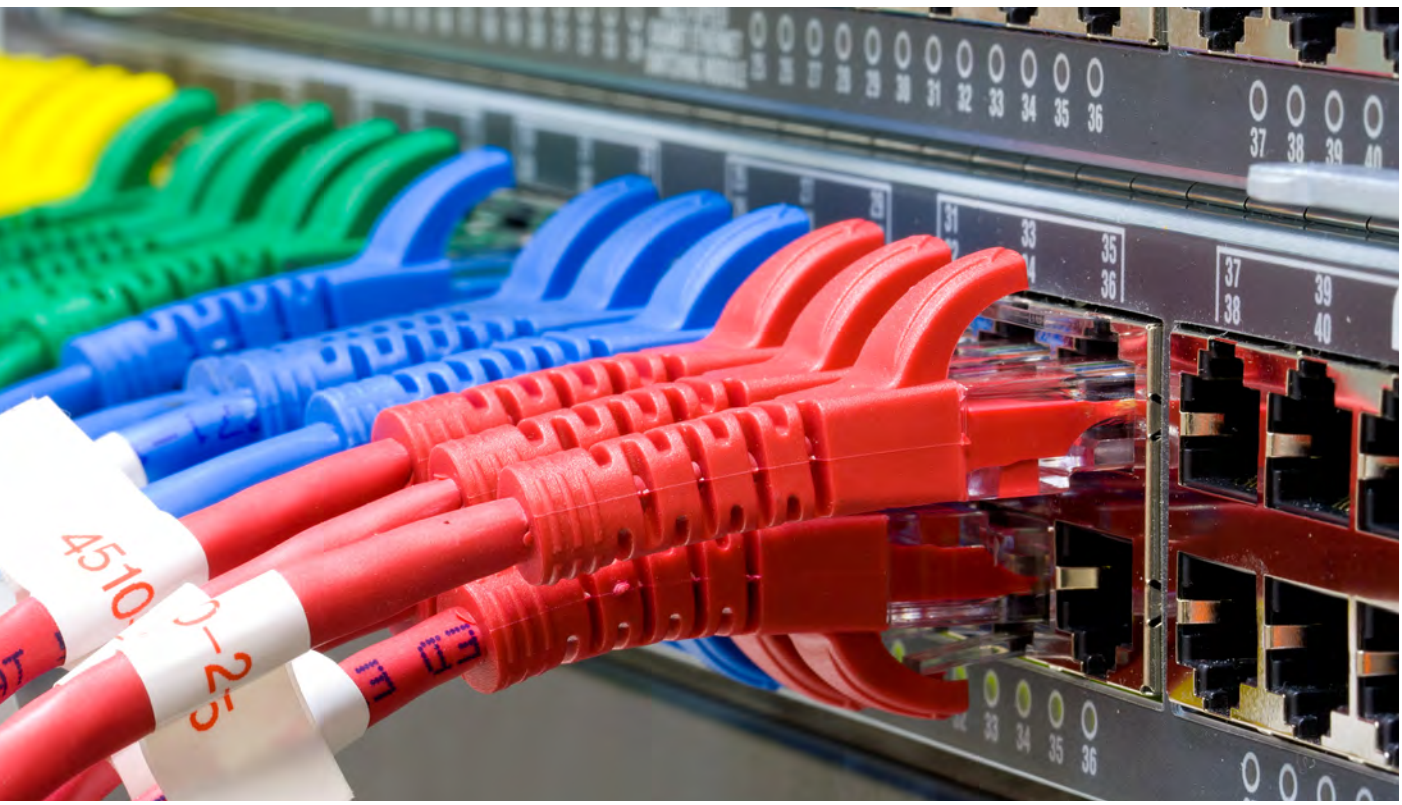
- Digital databases
- Digitization of records
- Secure data exchange solution
- Digital information assets management
- Digital identity and digital signature
- Digital documents exchange
- Government portal
- Mobile messaging gateway
- Payment gateway
- Cloud computing
- Privacy and security
- Cyber security
- Telecommunication networks
- Sector solutions

Key analog elements of e-government

- Legislation and regulations
- Cooperation with businesses
- Supportive organization
- Financial models
- Political will
- Change management
- Awareness raising

Plenary Hall of the Estonian Parliament (Riigikogu).

Digital elements of e-government



Digital databases

Databases are the backbone of government. Governments use data for various purposes: to maintain an overview of the population, to issue identity documents, to register, tax and monitor business activities, to organize land and property ownership and others. Databases provide detailed information about the registered objects (land parcels, houses, vehicles, etc.) and allow governments to register and identify their owners. Registration in a government registry usually serves as proof of ownership of the land, property, business or vehicle.

High-quality databases are also a great source for understanding the bigger picture. A civil registry with good-quality data on the population aids in the understanding of changes in population trends, by both age group and location. Registry analysis of vehicles, for instance, helps understand wealth trends in the population — if individuals are registering more new cars than before, probably their wealth, income and faith in the future are all improving.

During the last decades, most governments converted their data from paper format to digital. Those that did not already are in the process of doing so.

Historically, governments kept their data in paper format. Now, most governments are capturing and stor-

ing data digitally. The technical tools vary, from simple office software spreadsheets to powerful, cutting-edge solutions. The main point is that e-government implementation requires the data in the registries to be maintained in digital format, as a computer cannot access paper documents that are stored in physical files in archives.

A country's primary databases should include these:

Civil registry (population register)

Real estate registry (buildings, land cadaster and property ownership)

Business registry

The names of these databases may vary, but their functions should remain consistent.

Main databases are usually kept at the national level, but in many countries data is collected and stored separately at the state, provincial and municipal levels.

The main registries, or first-tier registries, are so named because most of the other registries take data from them. The second-tier registries capture specific data and usually bind it with data from the main registries.

If to look at the example of a national database of vehicles, it collects specific information about cars, trucks and busses, connecting them to their owners. Ideally, a vehicle's data is connected to an individual's personal ID number (single identifier), and from the ID number it is possible to see all data about the individual that is in the civil registry. It means that the vehicle registry itself does not need to collect the individual's data — name, date of birth, home address — but can retrieve it from the civil registry and enter it on a given application form.

Main registries provide a single identifier for every person, business, parcel of land and business, usually in the form of a numeric code. The single identifier for a person is usually called a "personal ID number"; for businesses, "business ID number"; and for real estate, "property ID number." This helps to differentiate people with the same name, keeps track of a company's records if it changes names, etc.

Some say that a person's name and date of birth are sufficient to identify him or her. In many cases, that may be so. But bear in mind that many countries use several languages, each with its own spelling rules. Some countries even use multiple alphabets. These factors create the risk that people may not be identified properly and their data is not recorded in the right place.

A single identifier numeric code is machine readable and allows computers to recognize and connect a person with the correct data.

Maintaining the high quality of databases and updating them continuously makes the civil registry a key information asset. Thanks to the data in this registry, the government can understand the demographics of the country and plan better healthcare, education and public transport. It can also use the civil database as the basis for a voters' registry and for other applications.

Digitization of records

If a database such as the population register is still in paper format, how to make it digital? Usually there are two strategies, deployed in parallel.

All new data is captured in digital format. This means that all family records (births, deaths, marriages, etc.) will be recorded in the digital population registry starting from a certain date.

All existing data is digitized. This means that existing paper documents are scanned, the data from the doc-

A single identifier numeric code allows computers to recognize and connect an person with the correct data.

uments is transferred either manually or by automated text recognition software to the database while using quality assurance measures. The digitization process goes systematically back in time. Data is captured step by step, from the newest documents to the oldest. At the same time, data is also captured from older documents by request, as in the case of marriage or death registration, etc.

Several countries and regions, including the European Union, are implementing a principle called "once only." It means that the government asks for data from individuals only once, and after that all government agencies share it. It also means that the government does not record the same data, such as a person's home address, in multiple databases, but rather in just one — the civil registry. When providing services, other government departments request the individual's address from the civil registry and no longer from the individual. The system reduces the burden on individuals and companies, and eliminates risks related to data duplication and quality. If a person's home address is recorded differently in two registries, how to know which record is correct?

Who owns the data of individuals and businesses? The individuals and businesses themselves. The government just collects and organizes the data.

Often governments do not want to reveal the data they store. This is the wrong approach. First, people have the right to know what data the government has collected on them. Second, giving individuals access to their data allows it to stay accurate since people themselves will correct mistakes.

Secure data exchange solution

If data is in digital format and transferred among databases, the data exchange must be secure.

A Secure Data Exchange Solution (often called an Interoperability Solution) is not a superdatabase that consolidates all data from other databases. The idea of a superdatabase is dangerous even though it may seem attractive to government since all data is easily accessible and in one place. But this come with high risk. Data can be destroyed, by either technical failure or attack. Data can be changed or copied illegally. While such risks are inherent to small databases, the risk of total damage to a superdatabase is tremendously higher.

Safe data exchange does not entail government departments sending copies of databases to each other on disks or flash drives. Data can get lost or compromised in transit.

For this reason, governments need secure data exchange models.

A proper Secure Data Exchange Solution should meet the following criteria:

- Both sender and receiver of the data are registered and verified. Both sides are identified through agreed-upon procedures and mechanisms.
- The data exchange is encrypted, ensuring confidentiality. If somebody tries to steal or copy the data while in transit, it will be unreadable.
- The data transactions are time stamped. A time stamp confirms the time of the data transaction. By time stamping the data, it is possible to later verify its original state.
- Electronic records are logged and archived to ensure a legal audit trail. It should always be possible to trace who did what.

Because a country's Secure Data Exchange Solution is one of the critical pieces of its information infrastructure, high-level requirements apply to the system:

There must be **no single point of failure**. Even if the electricity goes off in a central government computer center, the system must be functional and available.

There must be legal meaning to data requests and answers. Data exchange must be supported legally since the manifestations of data exchange appear in everyday life. If somebody is selling a house, title can be verified through the property registry. If the transaction is digital and later a dispute arises, the parties must be able to verify that the owner is the seller.

Digital information assets management

Together with a Secure Data Exchange Solution, a country should establish digital information assets management.

Digital information assets include:

- Information about databases (registries)
- Information about services
- Information about user rights

Digital information assets are managed in the central registry.

Information about databases allows the government to monitor in which registry which data is recorded and accessible. This part of the central registry is called the "registry of databases metadata." This registry does not collect any actual data but rather records types of data such as "car license plate number," "passport number," etc.

Information about services is stored in the services catalog. It contains descriptions of all online services and uses data from other databases. It also records the legal basis for services. To ensure security and privacy, all services must be approved before launch by an independent data-protection and digital-security authority.

Information about user rights is also stored in the services catalog. It defines machine-to-machine user rights, provides access to registries and other databases and collects information for services.

Digital identity

Digital identity moves traditional physical identity into the digital world.

We are asked to prove our identity in all kinds of situations — when entering offices, making payments, crossing borders, submitting applications for government or business services, etc.

In the physical world, identity is usually confirmed by comparing the photo on an identity document (passport, ID card) to the person's face. In the virtual world, parties do not always see each other, so they need other means to identify themselves, be they citizens, clients or customers.

Because of emerging online services, digital identity is becoming more and more relevant. Both governments and businesses are seeking ways to identify their constituents and clients in the online world.

There are two main functions of digital identity.

First, to **prove your identity in the virtual sphere** so that the computer system with which you interact recognizes you as a user (such as a bank customer) and associates you with your user account (such as your bank account).

Second, to **verify virtual transactions** such as bank transactions, government service requests, internet purchases, etc.

There are two main options for developing digital identity.

The first option is **digital identity developed by the individual**. People increasingly depend on internet access and are able to assert their own identities in digital form.

Google, Facebook and Microsoft together facilitate over one billion "identities," a number that is surpassed only by the combined populations of China and India. Facebook penetration rates in some sub-Saharan African countries are higher than birth registration rates. People constantly create new online identities to buy tickets, make purchases, receive news, etc. This option does not depend on a connection to a physical identity.

The second option is **digital identity securely connected to a physical identity and trusted by the government**.

Estonian national e-ID card

These two types of digital identities are not at odds. There is a place for each. In contexts such as Facebook or Twitter, an individual presents his identity as he wishes, and there is no obligation on the part of other users or organizations to trust this identity. It can also be used by means of verification. For example, if someone pays to access internet content (music, movies, other entertainment) and connects the payment information to his Facebook identity, that is sufficient for the content provider to allow further online access. It need not develop its own system of usernames and passwords.

For governments, the extent to which such "self-declared identities" are recognized remains an open question.

There are other options that fall somewhere between the two mentioned above.

For online clients, financial institutions usually provide their own means of digital identity, as they require much more confidence in online transactions. Also, banking rules demand financial institutions to "know your client." For transactions with government, the kind of identity provided by banks is much more acceptable (but only if the government truly believes that banks know their clients).

A strong and trusted digital identity should be provided by the government. And the identity should be based on proper population management and civil registration.

A strong digital identity is an extension of traditional identity. The instruments of digital identity — electronic ID cards, smart ID, mobile IDs — are new types of documents, allowing individuals to act in the virtual world.

Traditional civil registration requires permanent and sustainable management and funding to stay relevant, accurate and up-to-date. There cannot be interruptions. Data constantly changes, as people are born, die, get married, divorced and otherwise change names on a daily basis. Proper registration allows for an ongoing and lifelong engagement with individuals which follows them from birth, through document issuance later in life, to death.

A digital identity can work only if supported by proper civil registration and a civil registry.

In recent years, many countries have undertaken the creation of a comprehensive, computerized civil register that is centralized and networked. Such a register is often known as the "national population register" or the "national identity register." It allows civil and other registration authorities, such as those registering residences and issuing passports, to use a single platform for collecting, processing and retaining personal identity information. The civil register serves as the backbone of a national population registration system. As part of the rollout of such a system, many governments have distributed identity cards to the population. The latest models of these cards are smart cards embedded with machine-readable chips that often contain not only the data fields visible on the card (including the person's photograph), but other data fields readable only by certain state officials (such as law enforcement officers equipped with handheld card readers).

A true digital identity is one that can be used securely online.

Types of digital identity:

Smart cards with machine-readable chips are the most common instruments of digital identity. Smart cards usually have a dual function. They display a visual identity — printed name, date of birth, photo, etc. — and they contain on their chip a digital identity — a set of data and software protected by encryption. To use a smart card, the holder must have a card reader for his computer and special software, usually free of charge and publicly available. The card itself carries a specific kind of individualized software, which is called a key.

To start a trusted transaction, the cardholder's computer must be connected to the internet. The cardholder identifies himself with a personal identification number (PIN). A series of automated queries, invisible to the cardholder, take place to make sure that the card is not blacklisted or closed and the certificates are valid. If there are no problems, the identity is approved and the user can start using online services.

A similar procedure takes place when a person gives a digital signature.

Many people around the world do not have access to computers but rather to mobile phones and mobile networks. Globally there are close to 5 billion mobile phone users. This means that almost the entire adult population worldwide has or will soon have a mobile phone. To recognize the user and the phone number, phones use SIM cards (SIM meaning Subscriber Identification Module).

Mobile ID is a solution combining the capabilities of mobile phones and digital identity. To enable mobile phones to carry a digital identity, an encrypted set of data and software similar to that used in smart cards is transferred to the phone's SIM card. The phone's keyboard is used to provide a PIN number, which activates the digital transaction and identifies the user. The transaction itself is visible on the phone's screen.

> A strong digital identity can work only if supported by proper civil registration and a civil registry.

The keys to success of a strong digital identity are proper population management and a high-quality civil registry. The critical step is connecting physical identities with digital identities. The same government agency should be responsible for issuing both physical and digital documents, which as described above, can take one form: the smart card.

Many countries are now issuing passports with a chip containing biometric data. The chip provides additional verification sources for border guards in addition to the visual data in the passport. However, passports containing digital information are not considered digital identity documents, as they do not enable digital transactions for the passport holder, who cannot identify himself or herself online nor provide a digital signature using just a passport.

Digital signature

The digital signature is one of the key elements of e-government.

A digital signature has the same meaning in the digital world as a handwritten signature in the traditional world. As we cannot sign documents on a computer screen with a pen, we need a more sophisticated solution.

With a digital signature, individuals and organizations can sign electronic documents, verify online transactions, etc.

A digital signature most often is used when there is a need to both verify a transaction (approve a bank payment, sign a contract) and memorialize it for the future (ensuring a contract is signed by both parties).

A valid digital signature gives the recipient confidence that the messages or document was created by a known individual, undeniably signed and not changed in transit. Usually a digital signature also documents the exact time of signing by including a time stamp.

Sometimes digital signatures are called electronic signatures. But there is an important difference. An electronic signature may simply be a name entered in an electronic document (such as inserting a handwritten signature image in a PDF document), whereas a digital signature is trusted by the government and protected by encryption.

For most governments' online services, it is sufficient to simply identify a citizen. In advanced countries, online services require digital identification, meaning citizens must sign digitally.

It must be emphasized that the use of digital signatures is not limited to transactions with the government. On the contrary, in countries that have taken to using digital signatures, most are used for either business-to-business transactions (signing contracts, delivery documents, etc.) or business-to-consumer transactions (sales contracts, service contracts, etc.).

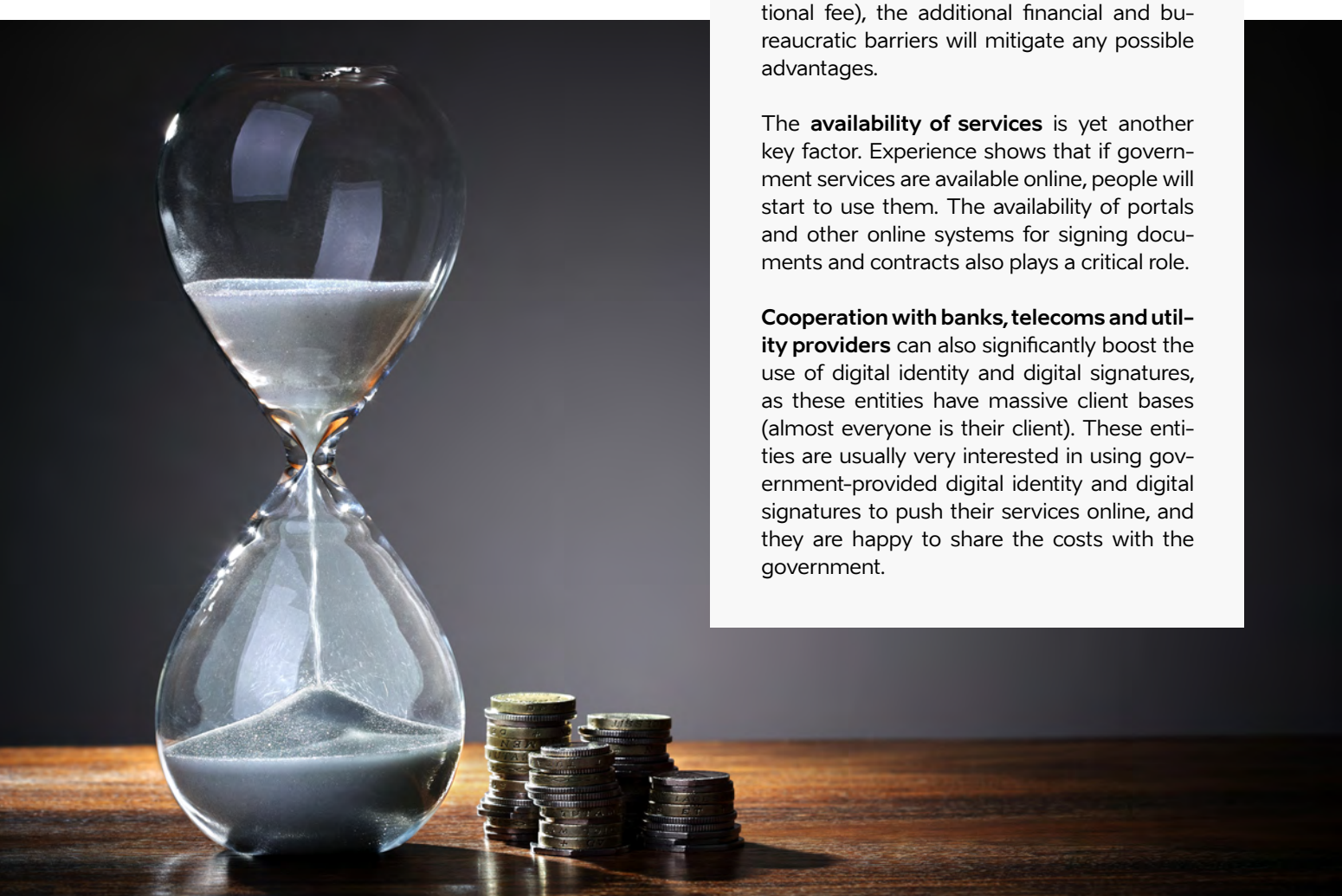
Success factors

Among all the technical and regulatory issues, the main questions seem to be how to make digital signatures easily accessible to the general population and what kinds of services can private people and businesses use with digital signature.

It appears that the **best model is to provide digital signature tools to the general population as part of the rollout of smart cards.** This means that digital signature tools are stored on smart cards, and people receive the tools bundled with the physical card. In this way, everyone has access to a digital signature but retains the choice whether to use it. If people must apply separately for a digital signature (and probably pay an additional fee), the additional financial and bureaucratic barriers will mitigate any possible advantages.

The **availability of services** is yet another key factor. Experience shows that if government services are available online, people will start to use them. The availability of portals and other online systems for signing documents and contracts also plays a critical role.

Cooperation with banks, telecoms and utility providers can also significantly boost the use of digital identity and digital signatures, as these entities have massive client bases (almost everyone is their client). These entities are usually very interested in using government-provided digital identity and digital signatures to push their services online, and they are happy to share the costs with the government.



Digital documents exchange

Digital documents exchange allows the secure and guaranteed exchange of digital documents among governmental institutions.

Government institutions develop documents in computers and, if they are advanced, in digital document management systems. But in the end, they still print out letters on official letterhead and send them by courier to other branches. When received, the letters are scanned and copies are circulated.

In better cases, electronic documents are sent by e-mail, but here too, both sender and receiver cannot easily ensure proper dispatch and delivery without manually confirming.

Digital documents exchange solutions solve these problems by providing guaranteed delivery and receipt of digital documents. It works like an address book. Once a document is created and approved, the digital office assistant selects from the system's address book the name of the recipient and sends the document as an attachment. The system provides a receipt of both dispatch and delivery.

> More and more these days, people use mobile phones and tablets to browse the web. Website development tools already allow for adjusting the presentation of a website according to the screen and browser being used. These adaptive solutions help those using small screens and mobile devices.

Government portal

The central access point to a government's online services is the government services portal. This portal acts as a central information gateway to all government services, both offline and online, although it is not necessarily the only access point to the government's digital services. To provide a good overview of services and not to confuse users with a maze of web pages, the best practice is to confine the portal to as few web pages as possible.

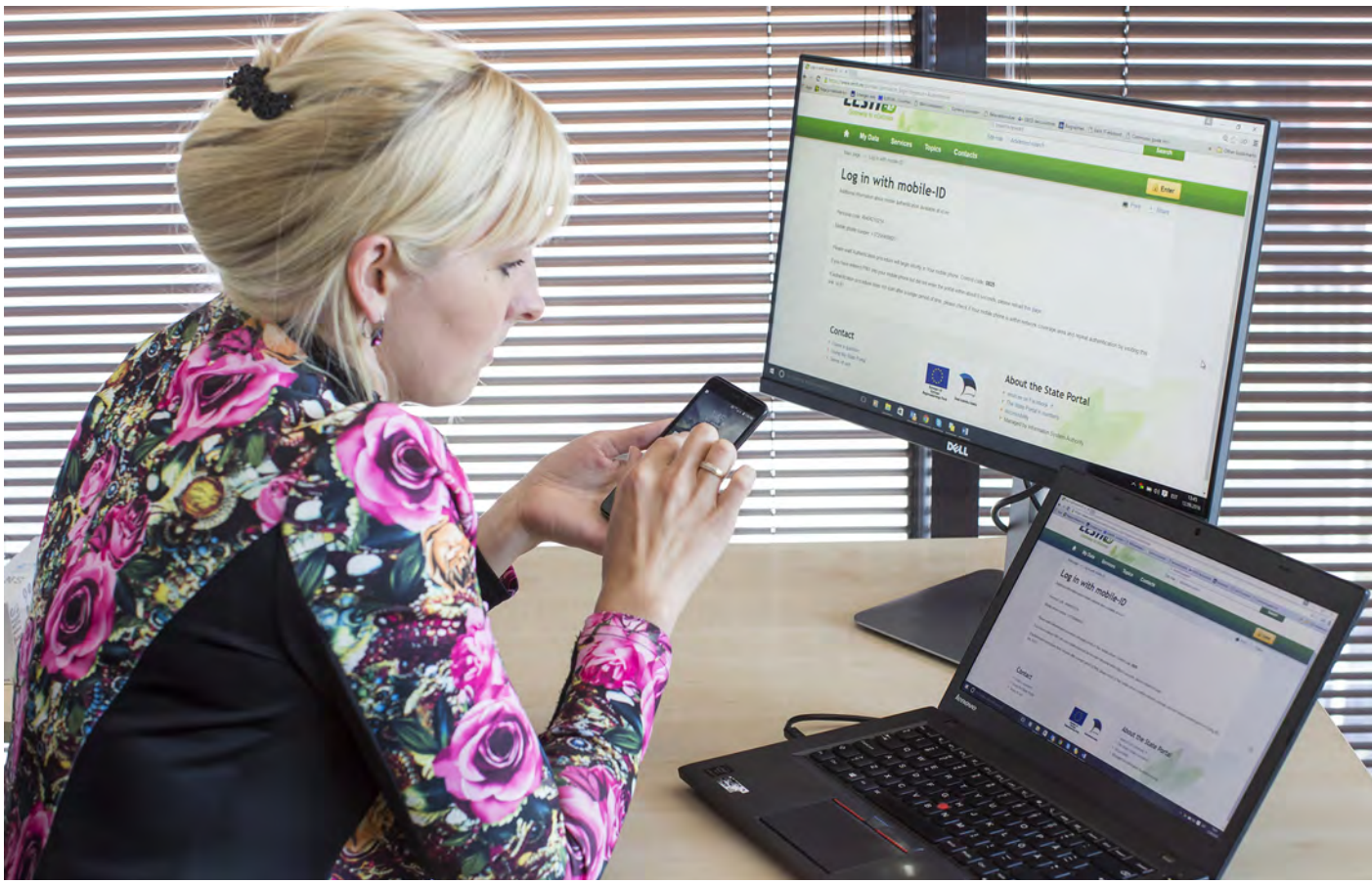
The value of offline information about services, i.e., written and non-interactive information, is often underestimated. This information should be clear, well organized and well presented. It should help individuals understand how the government can assist them in various situations: registering a birth, getting married, finding a job, visiting the doctor, applying to university, selling a car, etc. Drafting these kinds of clear informational texts is an art form in and of itself.

A typical problem for government is how to describe its services in a way citizens can understand. Here is an example. A person living in the countryside does not have enough money. In describing its response to that problem, the government writes about "measures supporting better access to resources in remote rural regions for citizens with limited financial literacy." Will the reader, who may have a limited education, understand what the available program actually is?

There are a multitude of governmental organizations within every country. Each tends to use its own nomenclature and develop its own online presence with its own look and feel. These individual websites may be quite nice, but they can be very different in style. Is this the single face that governments are looking for?

In countries around the world, governmental agencies are increasingly using similar layout and lexicon on their websites, supported by visual and technical guidelines. The websites usually are based on a uniform technical platform, but not always. Content development remains the domain of a given ministry or agency, which is close to information resources.

It is also worth considering how many websites a government needs. With great effort, the UK has managed



to reduce the number of central government websites from 474 (in 2013) to 281 (by the end of 2016).

The harmonization of online texts explaining government services is another huge task, demanding both dedication and cooperation within the government. Several governments have developed guidebooks to assist officials and to provide best practices. Some governments provide a central help desk during the transition period. Achieving this goal requires the definition of tasks, the implementation of timelines and the allocation of resources.

From the technical point of view, government portals are usually divided into two layers: a presentation layer and a services layer.

The presentation layer supplies visual information about services.

The services layer enables the use of services through an application template, data queries and submission. If separated properly, changes to the visual layer (new graphics, new text) do not affect the portal's technical operation.

More and more these days, people use mobile phones and tablets to browse the web. Website development tools already allow for adjusting the presentation of a website according to the screen and browser being used. These adaptive solutions help those using small screens and mobile devices.

For the foregoing reasons, it is never too early to start developing a government's main website. Although the first online services may be ready only after a year or two, organizing the information should start without delay.

Mobile messaging gateway

To benefit from the widespread use of mobile phones and to ensure the fastest possible dissemination of messages from the government, it is necessary to develop mobile messaging gateways. **The main function of a mobile messaging gateway is to enable the sending of short messages (SMS) to mobile networks directly from the government portal.** A typical example would be when a government office has prepared a document — for example, a renewed driver's license, which is ready for pick-up. Sending an SMS is a convenient and quick way to inform the recipient. As we know, most people have their mobile phones with them at all times. This kind of service could be in addition to notification by e-mail.

A mobile messaging gateway also allows the sending of bulk messages to the population of a certain area — for example, in the event of an emergency or natural disaster.

The main technical feature of a mobile messaging gateway is its ability to translate e-mail-type messages to SMS-type messages, while coping with the fact that the involved technologies can vary.

Payment gateway

A payment gateway allows governments to receive online application forms together with the associated fee.

A government charges fees to individuals and businesses for most of its services. If an application is submitted by hand at a physical office, a desk clerk usually collects the fee, either by cash or credit card.

For online services, a similar procedure takes place. At the final stage of an online application submission, the payment gateway seamlessly generates payment links to the applicant's bank, mobile payment provider or credit/debit card processor. The user selects the desired payment method, and the payment gateway executes the payment with all necessary affiliated information. After the payment is successfully executed, the gateway sends a confirmation to the government office.

A payment gateway speeds up the delivery of government services. Although the money being transferred from the individual's bank account to the government's may arrive a few days later, the bank or other financial institution can confirm and guarantee payment immediately, allowing the government to provide the service without delay.

Cloud computing

Cloud computing is a type of internet-based computing that provides shared computer-processing resources and data with computers and other devices on demand.

The most well-known and popular cloud computing solutions are, among others, Gmail, Dropbox and Flickr, which allow users to store and share their data online. This is helpful when the user does not possess any large-scale physical computer infrastructure (server, data storage, data processing capacity) on its premises, and so the physical infrastructure exists somewhere else — in "the cloud." This off-site service dramatically reduces investments in datacenters, hardware and software and reduces staffing costs.

Cloud computing offers many advantages to governments, businesses and consumers, such as cost-effectiveness, flexibility, scalability and faster development and testing of new solutions which enable innovation. Several countries already have an agenda for developing cloud computing for government and are actively taking steps towards implementing it. For government, cloud computing offers better services with fewer resources.

Cloud computing technology is already fairly mature. For government, there are two main problems: the physical location of data and the availability of data.

In many countries the law requires the government to store its data within the country's physical territory. There are reasons for this. With Gmail, Flickr and the like, we do not know where the data is actually located, as these companies maintain datacenters around the world. For storing someone's holiday photos, this is fine. But if the data comprises a country's national civil register, then its location can become an issue because law enforcement agencies may have the right to demand access to data that is stored within their country's borders. And they do not care to whom the data belongs.

Another issue is data availability. Critical data such at that in the main registries should be available 24/7 without hindrances or delays. In the event of a cyber attack against a country, for example, international internet connections likely would be shut down right away to prevent further attacks. In this case, data would not be retrievable from the cloud.

One solution to this challenge is creating a government cloud.

A government cloud, physically located inside the country, would ensure convenient and secure cloud solutions for government institutions and providers of vital services. The government cloud could be set up and run by the government itself or by private entities or based on a hybrid model. If set up and run properly, it can provide services efficiently and secure real savings.

Privacy and security

Owing to the ever-increasing possibilities for using information technology, privacy of individuals as well as security and integrity of data must always be on the agenda.

The challenge of digital privacy might be addressed as follows:

Since governments collect large amounts of data from individuals and organizations, there must be mutual trust between the government and the data owners, i.e., individuals and organizations.

Governments have an interest in motivating data owners to provide correct and up-to-date data. And both sides are interested to ensure that data is maintained and managed securely.

The following principles should be considered and implemented:

- **Confidentiality** — data should be stored and protected properly, and only authorized persons can access it.
- **Integrity** — data is recorded as presented, only authorized persons can make changes and changes are traceable to the person who made them.
- **Accessibility** — data is accessible for services without hindrances and delays.

Cyber security

Cyber security doesn't exist in isolation. It is a fundamental part of e-government development and supports digital innovation. Cyber security is not a brake that slows digitalization but rather a throttle that makes rapid digital innovation possible.

Cyber-security-related risks are growing rapidly. Some cyber incidents are caused by human error or technical failure. Others might be organized by criminals or terrorists. Governments might use cyber offensive capabilities as part of special military operations. These threats directly affect the normal functioning of national information and communication systems and, through those ICT systems, electronic services such as passport, migration and customs controls at borders.

The same threats may also affect general critical infrastructure and essential services — for example, electricity production and distribution, drinking water and sewage systems, gasoline station sales and pumping systems, supermarket cash registers, bank machines and many other systems that use internet and ICT tools to operate.

If such critical systems or essential services do not function properly, a country's government, economy and lifestyle can be adversely affected.

To be prepared for these risks, governments are developing national policy frameworks for nationwide cyber security. Those frameworks help define how cyber security related activities should be organized and how roles and responsibilities among institutions should be shared.

To manage cyber threats, countries must have appropriate laws and government entities that are responsible for baseline cyber security and incident management. There must be laws and agencies specifically for combating cybercrime and cyber terrorism. In addition, military forces should have the capability, manpower and supporting legislation to protect national cyberspace. In other words, cyber security must be integrated into the national safety and security system.

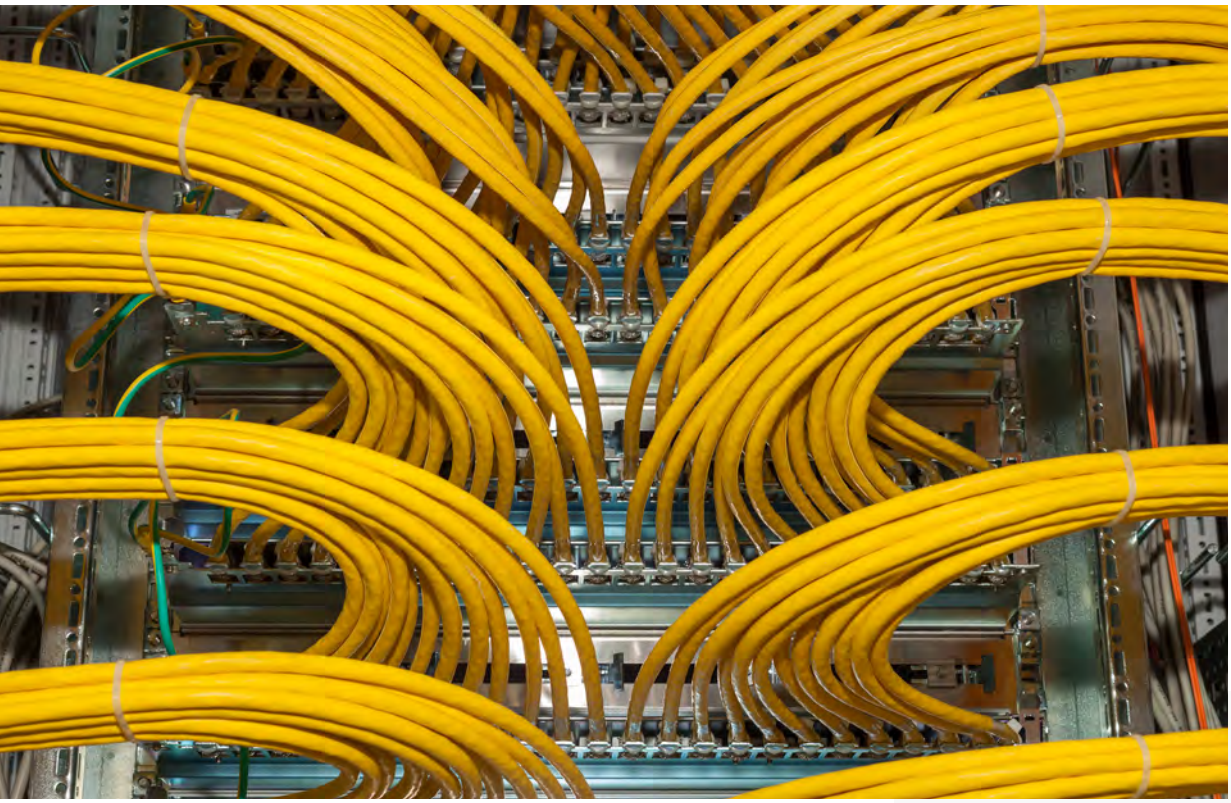
Baseline cyber security entails government officials' digital behavior, which is a critical factor. It involves not only access rights and secure logins to government databases, but also visits to suspect websites from government computers and even just locking the computer before going on lunch break. It means establishing a healthy cyber security culture.

A healthy cyber security culture should be created at the organizational level because every organization has a role to play in ensuring cyber security. Organizations manage work processes and also the ICT systems that support those processes. This means that organizations must analyze cyber risks and take measures to minimize them. The goal should be preventing cyber incidents by implementing information security standards and procuring ICT systems that are secure by design. It is also important to teach employees how to follow cyber security basic rules and to create procedures and capabilities for incident management.

At the individual level, a significant cyber security risk is theft of digital identity. It may take the form of an attempt to steal an online account holder's financial or other information, known as phishing. This most often occurs by means of sending fake official-looking emails to people asking them to send, for example, their banking login information.

Another scenario involves taking over someone's social media or email account and using it to send inappropriate messages or harass people including the embarrassed account owner. Although such incidents may not cause economic harm, they can damage social relations, cause emotional distress and even induce suicides. Loss of digital identity and account takeover risks are particularly high when computers are shared, such as in schools, at public internet access points or even among a family at home.

To deal with the problem, it is necessary to make individuals aware of these risks from an early age. The challenges, risks and mitigation strategies should be discussed in schools and in public media. Many countries have created a dedicated web police officer position (sometimes called a web constable) within the police department. These officers are available 24/7 to respond quickly to citizens' requests for assistance with incidents of identity theft, harassment in social media, etc.



Telecommunication networks

Providing access to the internet is a key factor for developing information society. It also serves as the foundation for delivering and using e-government services.

Internet access is usually provided by telecommunication companies, who run telecommunication networks. Internet access can be provided either by wired networks or mobile networks.

In the case of a wired network, the computer or other device is connected to the network either directly by cable or by having the last few meters at home or in the office covered by a wireless access point connection (WiFi).

In the case of a mobile network, devices use mobile phone technologies connected to a mobile operator's network.

> Providing access to the internet is a key factor for developing information society.

For a better understanding of the structure of telecommunication networks, we can look at the nature of those networks as provided below.

The next generation broadband network is geographically made up of three distinct parts:

- National backbone network
- Regional backbone network (middle-mile, backhaul)
- Access network (last-mile connections)

The national backbone network connects the regional backbone networks in cities and metropolitan centers. The equipment used in the national backbone network makes it possible to transport and exchange large amounts of data among different locations and operators.

The regional backbone network connects several access networks aggregating the local traffic further up in the network. It is the connecting link between access networks and the national backbone network. The regional backbone network also connects network devices in a given region to each other, allowing data traffic to flow among them.

The access network is the closest to the consumer and connects the consumer's devices to the connection point of the nearest regional backbone network. Access networks can be divided into two: wired and wireless.

Wired networks

The last couple decades saw the development of various technologies (e.g., xDSL, vectoring, GFast) that made it possible to transport more data with higher quality through **copper lines**. As a result, the transmission capacity of copper cables dramatically increased. Unfortunately, development in this area reached the point at which the laws of physics prevented further advances, meaning that further increases in data transmission capacity via copper over long distances were no longer possible.

The spread of the internet also led to the adoption of technologies such as Docsis, which made it possible to transport data via **cable TV networks (coaxial cable)**. This technology created competition among telephone companies in regions that had a cable TV network. Coaxial cables boast a larger transmission capacity than copper lines, but a cable TV network is a shared network among consumers. For this reason, today's cable TV networks use coaxial cables mainly for networks inside buildings. The parts of the network located outside have been replaced with fiber-optic cables.

Access networks with the greatest transmission capacity and the best quality use **fiber-optic cables**. The limits on transmission capacity of fiber-optics are still not known, as laser technology keeps developing and light can transport increasing amounts of information. There are several types of fiber-optic-based access networks, whose common name is FTTX (fiber to the x).

Wireless networks

Wireless access networks are mainly meant for connecting the mobile devices of consumers. Some wireless technology is also used to connect buildings in locations where construction of a wired network is not possible. The main advantage of a wireless access network is that it is cheaper to build. Several different technologies are used. Some technologies (e.g., Wimax, WiFi, CDMA) enable point-to-multipoint connections, which feature a base station that can be used by several users at the same time. Some technologies (e.g., radio links) enable point-to-point connections. Radio links require direct visibility, which means that using them in forests and mountains may be problematic.

Mobile wireless access connections, or mobile networks, are mainly meant for connecting portable devices (e.g., mobile phones, tablets, etc.) to the internet. Mobile network technology is developing constantly, resulting in better and better connections. Today, mobile communication generations (e.g., NMT, 2G, 3G, 4G, 5G) are upgraded more frequently than ever before. Radio waves guarantee data communication in mobile networks. Because only a limited number of radio waves "fit" in the air without interfering with one another, an international agreement has been concluded and establishes which radio frequencies can be used for mobile communications.

In each country, the government has the right to control the use of radio frequencies (the spectrum). For this reason, the use of the spectrum is regulated, and in several cases it is also licensed (mobile networks spectrum).

E-democracy

The essence of e-democracy lies in the support and enhancement of democratic processes and democratic institutions by means of technology. It offers citizens an additional opportunity to participate in political processes. It does not replace traditional, offline democracy but has the potential to enhance and advance existing traditional democratic processes.

E-democracy is an integral part of e-government. We must not lose sight of a balanced development of e-governance, wherein e-democracy receives due attention along with e-administration and e-services.

Areas of e-democracy include the following:

- E-participation
- Government-to-citizen G2C
- Citizen-to-government C2G
- Citizen-to-citizen C2C
- Grass-roots activism and social networking
- Political campaigns
- Online media
- I-voting

Mechanisms for executing e-democracy include e-petitions, online consultations and crowd-sourcing platforms, among others.

E-petitions

E-petitions are an easy way to make sure that citizens' concerns are heard by the government. An e-petition expresses a point of view, usually on matters of public policy, and contains a request for action, or in some cases, inaction.

The branches of government to which e-petitions may be submitted should maintain rules governing the submission of e-petitions.

In Australia the right to petition parliament has been one of the rights of citizens since federation, and it is the only way an individual can directly place grievances before parliament.

The process for creating and submitting an e-petition in Australia is as follows:

1	You create a petition	Briefly describe your issue	Request an action from the House	Provide your details
2	We check your petition	**Form** (does it have everything it needs?)	**Content** (is it an issue for the House?)	**Language** (must be moderate)
3	Your petition goes online	People sign your petition	You promote your petition	More people sign your petition
4	Your petition is presented	Your petition is presented in the House	Your petition may be referred to a Minister	The Minister should respond within 90 days

Online consultations

Online consultations, or e-consultations, refer to the exchange of opinion between government and citizens via the internet. Online consultations are one form of online deliberation. As with any other consultation, there must be clear rules in place about the duration and format of the consultation. Additionally, the process by which the public's opinions are considered, accepted or rejected should be explained by the body providing the consultation. Online consultations afford a variety of options for presenting explanatory information: videos, photos, presentations, charts and illustrations can all help the public, as well as stakeholders, understand an issue and formulate feedback.

Crowdsourcing

Crowdsourcing refers to the process whereby direct input comes from citizens. Online crowdsourcing allows citizens to share their ideas, deliberate and vote online. Prevailing ideas can then be submitted to the appropriate branch of government for implementation.

In Finland, the Open Ministry (Avoin ministeriö), a non-profit organization, has developed the online platform http://openministry.info/ for collaborating, sharing and signing citizens' initiatives.

Finland adopted a national citizens' initiative law on 1 March 2012, just one month before the EU Citizens' Initiative.

The main requirements for an initiative are as follows:

- 50,000 electronic and/or paper signatures by Finnish citizens of voting age
- 6 months for collecting signatures
- No pre-registration (in contrast to the EU Citizens' Initiative, which requires registration prior to collecting signatures)
- Can be either an agenda item or a law proposal (if in the form of legal text, it will be treated as a bill; if meant to start drafting legislation, it will receive a full reading in a plenary session of parliament, which will decide whether to accept or dismiss the initiative)
- Statements of support are accepted and should be certified by the Population Register Center
- Referendum not allowed, as parliament retains final authority to decide on the initiative

The Open Ministry's mission is to help citizens develop initiatives, to foster collaboration among the citizenry and to help put them in an appropriate format with the assistance of volunteer lawyers. The 50,000 signature requirement is not easy to reach unless a campaign is well prepared. The requirement was set to eliminate the risk of low-quality initiatives damaging the reputation of the whole system. Initiatives thus must be as good as possible to ensure that parliament takes them seriously. The Open Ministry team has been involved in most of the initiatives that have reached the 50,000 signature mark. Thus there is a clear correlation between support and outcome.

Participatory budgeting

Participatory budgeting (PB) refers to citizens' involvement in budgetary procedure. As a rule, parliamentary and municipal bodies decide on an annual budget, and the involvement of citizens is only through their elected representatives. PB allows citizens to directly vote on the allocation of certain parts of the national or municipal budget. Today there are already at least 1,500 instances of PB worldwide. In many places the entire process is conducted online. The best models, however, combine both online and offline tools.

City of Tartu, Estonia

The PB model in Tartu as well as in other Estonian local governments, with mostly minor procedural differences, consists of the following stages: first, local authorities decide on a specific amount of money from the local investment budget to be available for PB[1]; second, ideas are gathered from the residents on how to spend the PB budget; later, the submitted ideas are analyzed in one or several phases, depending on the municipality; next, the residents vote on the selected ideas; and finally, local authorities begin implementing the prevailing idea. The second stage, gathering ideas, can be divided into several phases: preliminary analysis of feasibility and subsequent open forums including public discussion and analysis by stakeholders. The submission of ideas as well as voting on them take place via e-tools.

[1] This can range from 150 000 to 5000 EUR.

Liia Hänni, the promoter of i-voting, is prepared to vote.

Internet voting

Internet voting (i-voting or online voting) allows voters to take part in national or local elections by casting their ballots online via an internet-connected computer or mobile phone from anywhere in the world. It is an additional voting method, used to improve accessibility to elections. It should not be confused with electronic voting systems or devices used at polling stations.

One of the main challenges of i-voting is identifying voters online. Several countries are experimenting with one-time passwords, available from the election commission before the elections and received by postal mail. Other countries are using government-trusted e-ID cards to identify the online voter.

Another challenge is safeguarding anonymity. This is usually achieved by the combined use of organizational, physical and cryptographic measures, allowing votes to be securely stored during the voting process and then afterwards irreversibly separated from the voter's identity.

There are many other new e-democracy tools, which if used effectively, can enhance interaction and cooperation between citizens and governments, stimulate citizens' political engagement and contribute to greater transparency and accountability, thereby enriching democracy.

Internet voting in Estonia since 2005

The Estonian solution is simple, convenient and secure, allowing voters to cast their ballots from a location of their choosing (home, office, abroad), without having to go to a polling station. There is a designated pre-voting period during which voters can log on to the system using their e-ID cards or mobile-ID to prove their identity. Later, upon casting a ballot, the voter's identity is removed from the ballot before it reaches the final counting stage, performed by the National Electoral Commission. Each vote thereby remains anonymous. After the online voting period ends, polling stations receive a list of confirmed online voters to prevent them from voting a second time in person on election day.

Internet voting was first introduced in local elections in 2005, and about 2% of all participating voters cast their ballot online. Since then, i-voting has been used eight times in Estonia, with the number of online voters increasing each time — 30% of all votes were cast online in the parliamentary elections of 2015, and votes were received from 116 different countries.

Further information:
http://vvk.ee/voting-methods-in-estonia/

Online procurement

Online procurement makes traditional procurement processes more efficient, transparent and accessible. Procurement fraud is one of the main forms of corruption in many countries, so every step toward transparency in the procurement process will save the public money.

Most governments begin by making it compulsory to publish procurement notices online, on a dedicated website. This step makes information more transparent and accessible, allowing companies from various regions access to the procurement.

More sophisticated online procurement systems allow potential bidders to receive automated notifications about procurements in their area of interest, download procurement documentation in digital format, submit clarification questions and make an offer. Government buyers can benefit from these systems by using a reverse-auction process, bargain for a final price and finally formulate all necessary documentation.

The Prozorro e-procurement platform in Ukraine

The **Prozorro** e-procurement platform represents a notable success story. Within its first 14 months of operation Prozorro became an efficient solution for the government, increasing transparency and reducing fraud. It resulted in the processing of over 100,000 tenders from 5,800 buyers and saving over UAH 1.5 billion in state funds. In 2017 another UAH 5 billion in state savings is expected. By the end of 2016 Prozorro's users totaled 19,000 suppliers and 60,200 bidders. The solution was scaled up nationwide and enhanced with expanded analytical and monitoring features.

Website: prozorro.gov.ua
Established: April 2015
Number of users: 19,000 suppliers, 60,200 bidders
Partner Institutions: DFID, EBRD, European Commission, GIZ, KMBS, Ministry of Economic Development and Trade, OSF, TI, USAID, WNISEF
Instruments created: public e-procurement platform, online marketplaces, DoZorro and BiZorro (public spending monitoring and control)
Time to develop: 3 months for MVP, 13 months for full scale system
Number of employees (team): 80
Cost: USD 500,000
Key achievements: UAH 8.8 billion saved, nationwide mandatory rollout
Key challenges: accountability and integrity of suppliers and bidders; level of professionalism of bidders; quality of monitoring and enforcement by government

Sectoral solutions

The above-mentioned digital elements serve as the foundation of e-government. On top of these basic elements there is the possibility to create an endless number of sectoral solutions, which can enable services in various areas: education, healthcare, law, economic development, agriculture, transportation, etc.

Typically, the development of sectoral solutions is the responsibility of ministries acting in accordance with the government's general political priorities.

Sectoral solutions can be supported with broader sectoral programs, such as for example, "ICT for Schools," "Mobile Solutions for Farmers," "Modernization of Public Transportation and Ticketing," etc.

Analog elements of e-government

Legislation

According to the principles of the rule of law, the governance of a country is conducted through legislation, and all activities, including those of government institutions, should be carried out in accordance with the law. Thus it would seem that activities related to e-government should also be governed through legislation. Yet it is not advisable to institute sweeping special legislation for e-government, as there can be a risk of creating a parallel system. This is not the intent of e-government, which should serve as a means to carry out regular government functions more efficiently and transparently. Developing e-government does not necessarily require drafting an inordinate amount of legislation. It does demand, however, that a country's legal system be assessed to identify areas in need of change or additional legislation.

It should be kept in mind that technology tends to develop much faster than legislation. It is therefore reasonable to adopt legislation that is technology-neutral — i.e., does not describe technologies — and leaves detailed regulations, where necessary, to secondary sources (government or ministerial decrees, etc.), which generally can handle change more rapidly.

It is important that the new ways of executing transactions through e-government do not lead to a legal vacuum. If there is uncertainty about the legal validity of a document or a signature, it will not be possible to transition to e-government. Electronic documents and transactions must be admissible as evidence in courts of law.

Legal organizations must be involved in developing e-government so that legal issues can be considered at every step. If regulations are enacted prematurely, new opportunities and innovations may be stifled. And if regulations are enacted too late, they may not adequately address online services. Thus the best practice is to develop legislation in parallel with technology and involve legal minds in innovation processes.

The regulatory framework should be clear and logical

to guarantee the stability of legislative development. A critical issue is balancing freedom of information with protection of public and private interests.

The principles of the legal aspects of e-government:

- Avoid over-regulation, as it risks creating parallel governance structures.
- Review existing legislation to ensure that e-governance methods are acceptable.
- Identify and determine responsible authorities, i.e., for carrying out reforms, monitoring the quality and accessibility of services, receiving complaints, etc.
- Formulate data-protection rules and a system of enforcement.
- Legislatively establish a secure form of online identification.
- Develop ICT and competition laws (sectoral and general) to ensure that proper access to the internet is secured.
- View e-governance as a tool for ensuring better access to information and fostering participation in democracy while bearing in mind that its technology is only a means to these ends.

Cooperation with business

The opportunities offered by e-government and information technology reach far and wide. While they are inherent to the ICT sector itself, they can touch all aspects of economic activity: industrial production, agriculture, transportation, services, healthcare and social works. The innovative approach and myriad applications of ICT can make the economy more efficient, productive, profitable and competitive in both local and global markets.

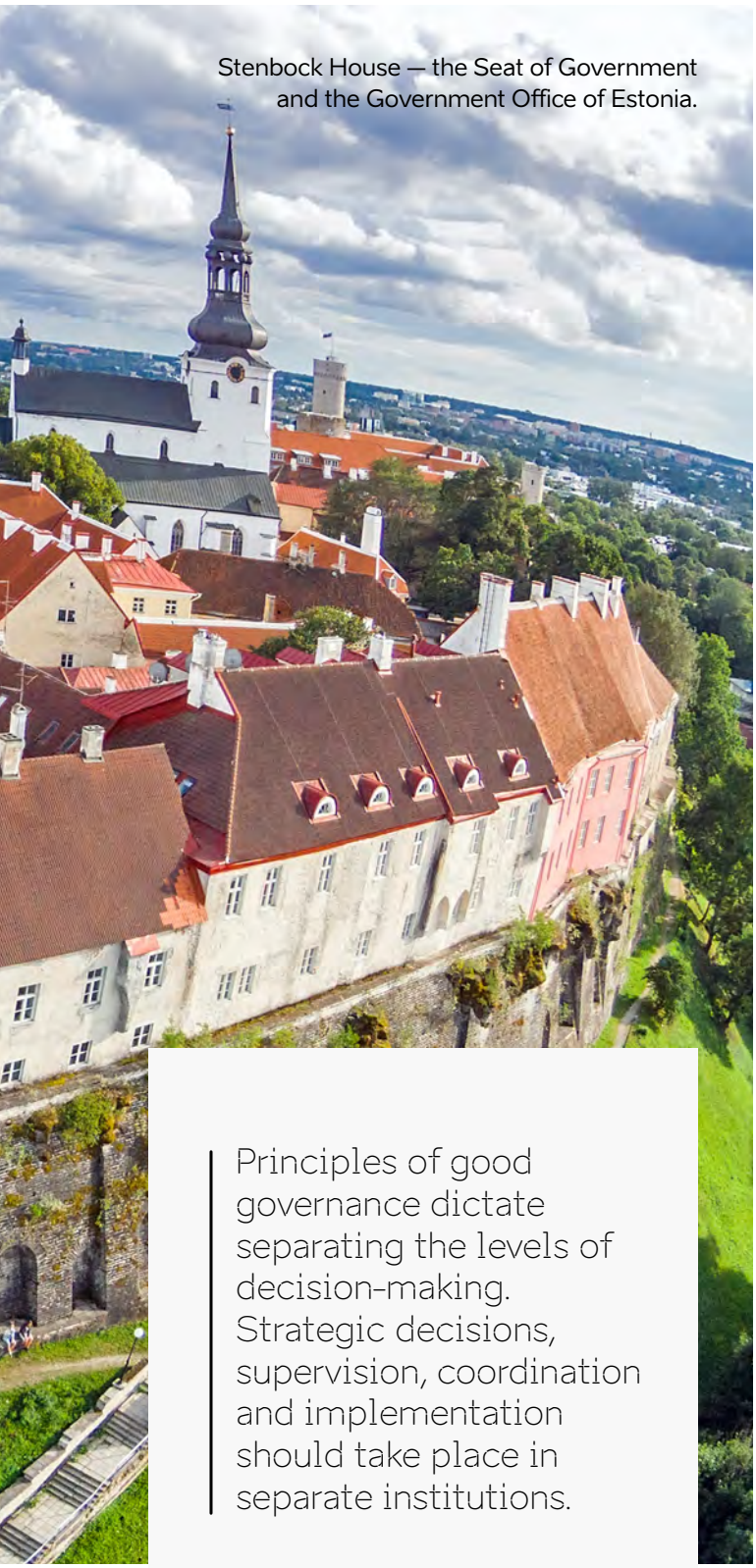
The ICT sector is critical to government and industry. It is local ICT knowledge, infrastructure and responsibility that support innovation, modernization and digitalization in both the government and the economy.

Developing a local ICT sector opens career opportunities, motivates students to strive for better education and creates new jobs and businesses, while requiring relatively small initial investment.

New procurement rules and their transparent implementation can boost innovation within government and bring cutting-edge technology solutions which can radically change paper-era bureaucracy and help move government into the 21st century.

Companies should be encouraged to invest in research and development activities and to be more competitive in global markets.

Business and governments should work together to promote digital literacy at all levels of society.



Stenbock House — the Seat of Government and the Government Office of Estonia.

> Principles of good governance dictate separating the levels of decision-making. Strategic decisions, supervision, coordination and implementation should take place in separate institutions.

Supportive organization

There must be **high level coordination of e-government activities** among the various departments of government.

Government institutions generally are keen to modernize their processes by using modern technology. The idea of coordination is not to centralize decision-making and technical capacity but to support innovation and the modernization of services delivery across all government institutions.

The tools for coordination are policies, legislation, regulations, budgeting, monitoring, common standards, allowing nationwide re-use of data, data exchange, re-use of software solutions and rapid development of online services.

Coordination of investments in ICT infrastructure and solutions is essential to avoid duplication and over-investment.

Principles of good governance dictate separating the levels of decision-making. Strategic decisions, supervision, coordination and implementation should take place in separate institutions.

There should be clear roles, mandates and responsibilities among institutions.

The parliament, president or cabinet ministers are responsible for approving the principles of information policy. Only these institutions can secure support for change at the highest possible level by taking strategic decisions and monitoring the progress of implementation.

The ICT Advisory Council functions as a consultation platform for stakeholders on all major initiatives, can resolve disputes and solve coordination challenges at the top leadership level. The council can provide guidance on matters that cannot be solved by agencies themselves. The official mandate of the council should be to decide upon and oversee e-government strategy and action plans, including their implementation. The body should include all ministers serving in the e-government sphere in addition to private experts from business, academia and NGOs.

The Central Coordination Unit might be either an independent agency or reside in the prime minister's office. The unit should have a clear mandate from parliament, the president or the cabinet. It should report directly to the prime minister to ensure that decisions and progress enjoy high-level political support and to assure access to resources.

International experience has shown that coordination activities conducted by the prime minister's office are much more efficient than if delegated to a ministry. There are several reasons. The issues that the unit deals with relate to a wide set of horizontal change management issues, which affect the entire government. All ministries (perhaps with the exception of the Finance Ministry) work in a vertical-hierarchical manner. ICT coordination should be conducted in a horizontal and networked manner. The prime minister's office also acts to "coordinate" political groups within government, helping to build consensus.

Ministries, departments and other agencies are responsible for their own working processes. They may choose to implement technologies by themselves while observing commonly agreed-upon principles.

The development of policies and standards should be centralized, while implementation should be decentralized. This means that the principles of information policy and its supporting legislation should be developed by the coordination unit, which works with stakeholders. Decisions relating to key investments and other large-scale financing should be coordinated in this unit as well. It is good practice to have the policy advisory council above the coordination unit, as shown below.

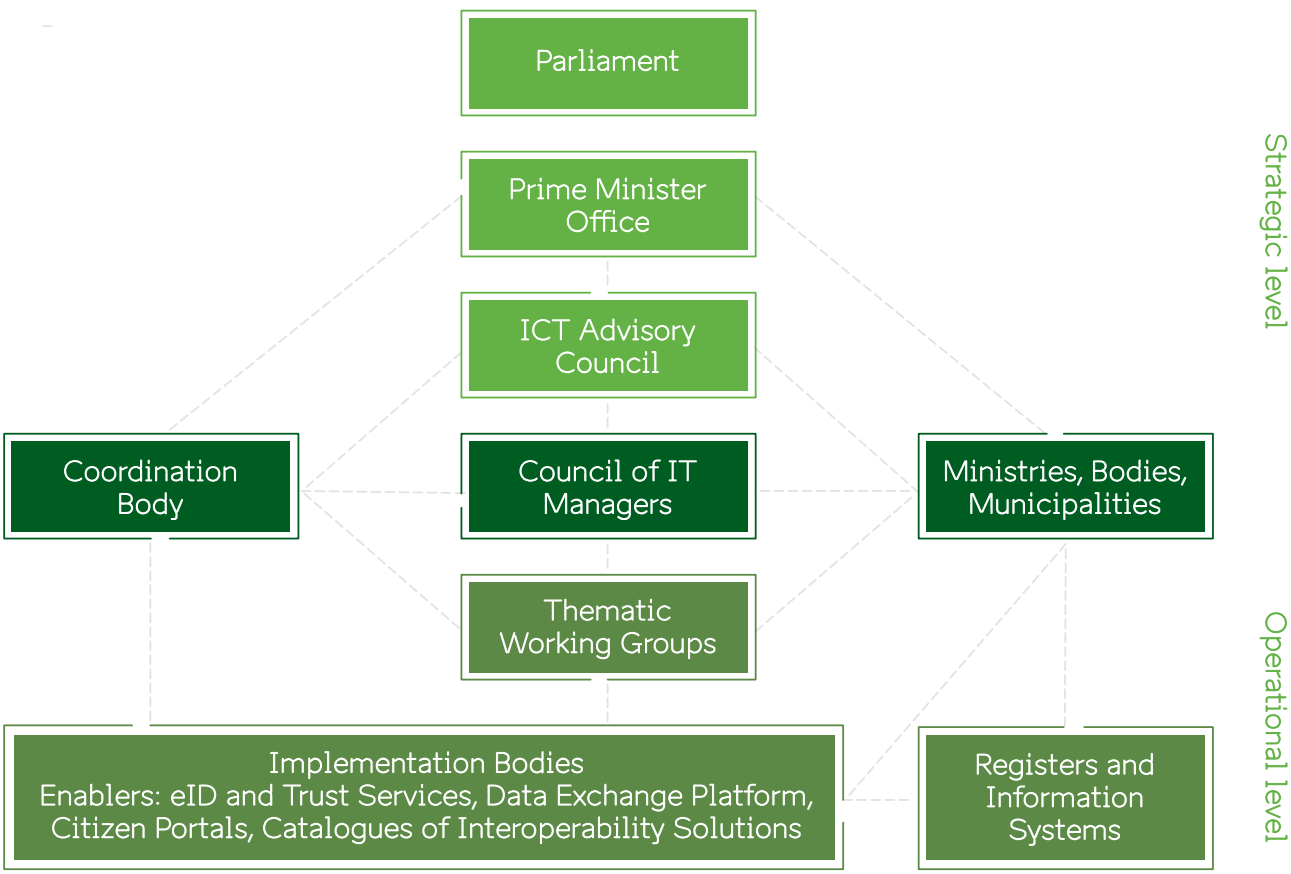


Figure 1. E-governance organizational structure and stakeholders at the interagency level

The Council of ICT Managers might serve as a central body of coordination, handling both strategy and operations. Its members would comprise cabinet members, department heads, chief information officers, chief technology officers and directors of ICT departments, in addition to outside experts from NGOs, academia, etc.

The council serves as the primary point of consultation on strategic e-government development issues by the ministries and agencies in charge of implementation. It also creates forums for technological discussions, sharing best practices and soft coordination of operational matters. It can also be used to collectively consult e-government stakeholders.

The Coordination Unit should serve as the secretariat and chair of the Council of ICT Managers.

Supervisory institutions monitor the implementation of legislation and regulations. Their scope of work generally reaches beyond e-government, and they deal with e-government issues from their own perspective. The main supervisory institutions for the purposes of e-government include the following:

- Data Protection Authority
- Technical Regulatory Authority
- Consumer Protection Authority
- National Audit Office
- Coordination Unit

The Data Protection Authority is responsible for private data protection. It monitors the legitimacy of the collection, sharing, accessing, publication and storing of private and personal data.

The Technical Regulatory Authority keeps an eye on radio frequencies/spectrum issues, monitors networks capabilities and oversees equipment conformity.

The Consumer Protection Authority is responsible for consumer protection in the spheres of telecommunications and internet access services.

The National Audit Office monitors the efficiency of government policies and programs and the success of their implementation.

The Coordination Unit acts as independent authority in some countries. It may have the right to supervise other government institutions when implementing policies and plans relating to digital security, the quality of online services, etc.

Other important stakeholders

- Universities and other research and development institutions
- ICT industry associations
- Software and hardware companies
- Banks and telecom companies
- Digital identity and trust services providers
- Open data communities
- Open source software communities
- Digital human rights groups
- Other community organizations

Financial models

A sustainable e-government needs sustainable financing.

Governments have experimented with various models of financing e-government. Here we describe financing options, not including those for telecommunications infrastructure, which often is accomplished by private entities using complex financing mechanisms.

Investments in nationwide solutions infrastructure

1. The government pays for nationwide solutions (hardware, software) from its investment budget.

2A. Running costs (maintenance, support, further developments) are covered by the government's running-costs budget.

    In this model, return on investment is not directly calculated. It is assumed that the solutions will boost the economy, reduce corruption and promote widespread efficiency.

2B. Running costs (maintenance, support, further developments) are covered by pay-per transaction fees, which are paid by government institutions internally.

    In this model, the "owner" is a government entity that counts the transactions (or other measurable units) and invoices the governmental institutions for their use. The model works when all government institutions have a sufficient budget for covering their costs. The risks of this model are that if funds are lacking at the end of the fiscal year, institutions may limit their transactions (such as data queries) to conserve money, and they may create duplicate databases to avoid paying for data.

Investments in sectoral solutions (law, agriculture, transport etc)

1. The government pays for sectoral solutions (hardware, software) from its investment budget.

2. Running costs (maintenance, support, further developments) are covered by the government's running-costs budget and service fees.

The government usually charges fees for the services it provides to consumers and businesses — registering or transferring the ownership of vehicles, registering a new business, etc. The running costs of providing those services should be calculated and included in the service fees. It is possible that during the first few years, when the use of online services is just beginning to grow, running costs will exceed income, but balance gradually will be obtained. For this reason, the government should play a balancing function by providing sustainable financing.

In general, the financing of e-government running costs should be kept at a stable level, and discussions about investment needs should be ongoing.

It is possible that during the first few years, when the use of online services is just beginning to grow, running costs will exceed income, but balance gradually will be obtained.

Saving money with e-government

It is also helpful to calculate the savings that e-government can generate for government, consumers and businesses.

Savings could be measured as follows:

1. **Time**. How much time was needed before, and how much is required now, to receive a given service, including the time it once took to travel to and from a government office (which is considered nonproductive). If we assign time a financial value (by relating it to the country's average salary) and then multiply it by the number of services provided, we can calculate the total savings for the nation.

2. **Paper, printing and other resources.** How much was spent on paper and the printing of applications forms and other documents versus how much is spent now.

3. **Erroneous payments.** Governments lose millions of dollars annually owing to errors in databases and the inefficient flow of information. They pay pensions to people no longer living, social subsidies to families with sufficient income, salaries to nonexistent government officials, agricultural subsidies to farmers for nonexistent cattle. Recovering these monies is usually next to impossible. These errors occur usually because of the low quality of databases and the very limited data exchange among institutions.

4. **Corruption.** Although it is difficult to calculate the share of governmental budget lost to corruption (since corrupt official usually do not declare their illegitimate income), transparent government reduces corruption and boosts the economy.

Additionally, governments can develop specific programs to support research and development related to ICT and e-government and stimulate cooperation between universities and businesses. The government can actively support these innovation processes not only through financing but also by laying the foundation for large-scale experiments with online services.

Political will

To secure long-term changes, political will and leadership are required.

Political leaders usually have lengthy agendas, so it is important to focus their attention on e-government issues, provide them with just the right amount information and keep them happy with quick victories.

Not all political leaders are aware of the potential of e-government. But within every government there are those who are enthusiastic about e-government and eager to support it. These leaders and their associated offices or ministries can champion e-government and inspire others to get onboard.

Consensus among major political factions within a nation's governing body is also important for fostering successful e-government. Since parliament is responsible for legislating, the critical mass of its members must be aware of the benefits, trends and progress of e-government within their country. This knowledge will enable them to support legislation that is essential for the establishment and running of e-government.

E-government should emerge as a top priority on political agendas. Political parties everywhere make pre-election promises about transparent governance, eliminating corruption, efficient public services and so forth. Such promises should be connected to plans for e-government. And hopefully these plans are later incorporated into the government's agenda for decisive action.

Last but not least, personal leadership makes a big difference, on both the political and administrative level. Committed leaders can accomplish a great deal even with limited resources by inspiring others and forming dynamic teams.

Estonian President Mr. Toomas H. Ilves is giving a keynote at Tallinn e-Governance Conference.

> The process of e-government implementation is about reinventing government. It is about change.

Increasing awareness

Vital to the implementation of e-government is increasing awareness of its potential.

Various factors can help people adapt to e-government solutions. Helpful measures can be taken in the following areas:

- **Cultural**. People may be used to the existing governance culture and prefer physical visits to offices and eye-to-eye contact with officials.
- **Economic.** Costs to access online services may be too high for some.
- **Religious.** In some religions, using numbers (such as personal ID numbers) instead of names for identity might not be accepted.
- **Security and privacy.** People may have concerns about how their personal information is collected, handled and stored.

There is no one right answer to each question for every country, as cultures, religions, histories and economies vary greatly. But all questions can and should be answered clearly — to the general public, stakeholders and experts.

As e-government provides a great deal of transparency, the implementation of its tools and programs must be transparent as well.

Change management

The process of e-government implementation is not only about technology and transferring services from paper to computer. **It is about reinventing public services.** To go further, it is about reinventing government. It is about change.

By definition, government is by the people and for the people. It also is run by people. To change the daily routines of the people working in government requires motivation. Some seek greater efficiency. Some want to see more data. Some want to provide better and more targeted public services. Some want relief from bothersome paperwork. Some are frustrated by the endless lines of constituents waiting for services. And some don't welcome change for any number of reasons — they may be near retirement, invested in a self-interested corruptive scheme or just lacking interest.

But government officials can be motivated. Change management is about releasing their energy and stimulating their ideas to re-engineer existing public services and related operations within government.

Government and its leaders must be able to change the mindsets of officials at all levels.

At a minimum, the government should seek to introduce the following:

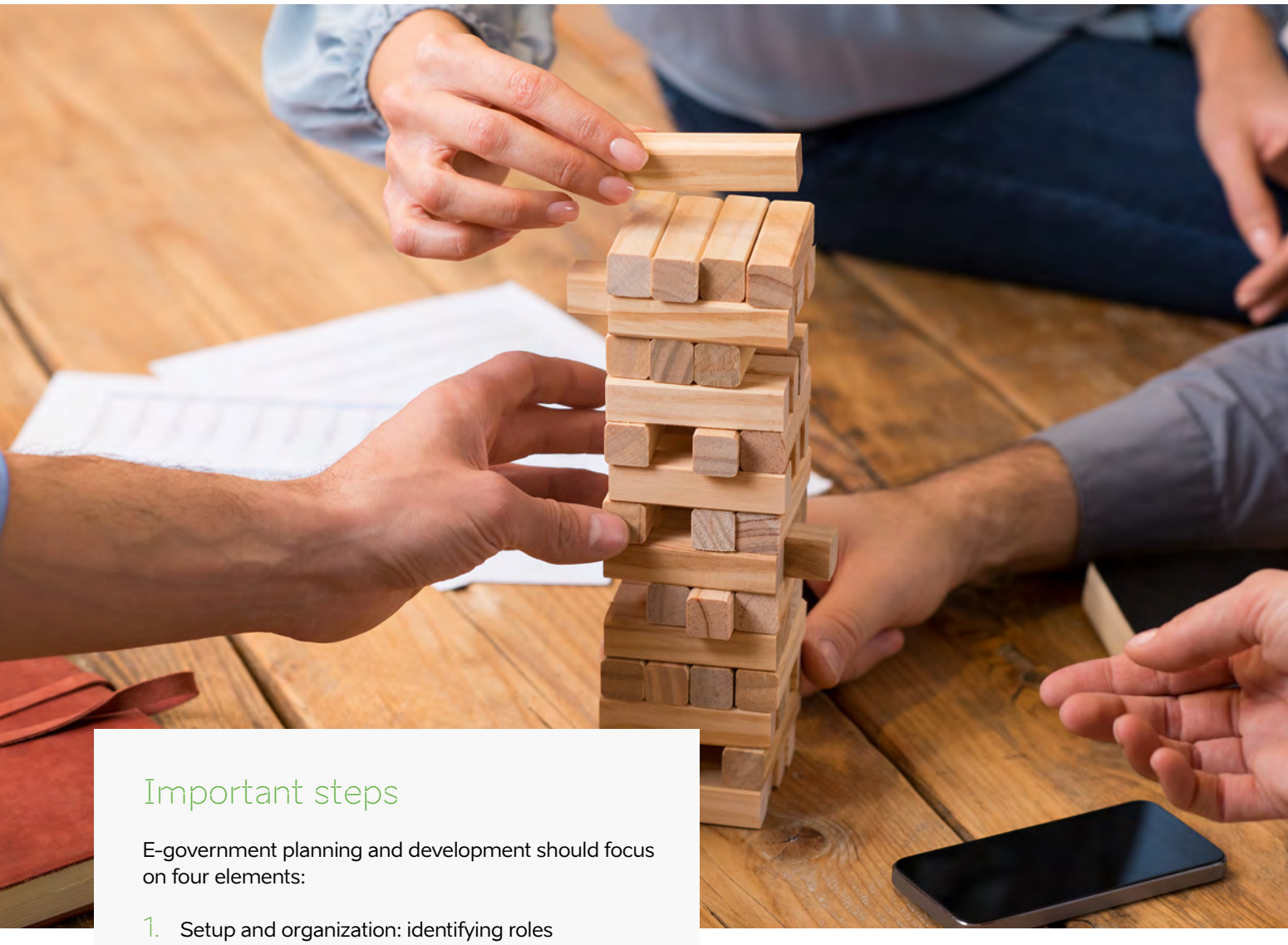
New skills

- Computer skills for common office solutions
- Computer skills for using sophisticated software (design, planning, technical design)

New abilities

- To analyze major data reflective of societal changes
- To understand the real impact of public services and collect and analyze related data
- To design new services according to new needs, based on high-quality data
- To design new services for delivery channels (online, mobile, kiosks)

E-government planning and implementation



Important steps

E-government planning and development should focus on four elements:

1. Setup and organization: identifying roles and determining responsibilities for coordination and implementation; encouraging public—private partnership and cooperation with academic institutions
2. Legal framework, strategies and action plans
3. General financing and financial models for e-services
4. Technical architecture and components

10 rules of e-government implementation

Rule 1:

The first thing first. International donors should not invest in technology implementation projects before the undertakings are thoroughly organized, plans are approved and sustainable financing is in place.

Rule 2:

General e-government architecture along with e-ID architecture should be developed at the same time as implementing service technologies. Building e-government from stand-alone services without an agreed-upon architecture is not sustainable, does not allow for sharing of data and can waste time, money and other resources.

Rule 3:

E-government cannot be imported. The knowledge necessary for planning, regulating and implementing e-government must come from within the country. Foreign experts come and go, but the responsibility for a healthy e-government remains internal. Local e-government leaders must be hungry for change.

Rule 4:

E-government implementation is about change management. Top government leaders must be engaged and recognize the need to change traditional business processes, regulations and data-sharing within the government. Clear strategy and sustainable organization are paramount. It should be understood that real e-government results can be seen only after several years of hard work. Political motivation, however, can be approached in the short-term and nurtured with small victories.

Rule 5:

Cooperation with the private ICT sector is critical. A model in which all ICT capabilities lie within the government is not workable or sustainable. Universities can lend support, but the main resource is private ICT companies, which work with ICT implementation on a daily basis.

Rule 6:

Start with pilot projects and "proof of concept" ventures to better understand needs and preconditions and involve stakeholders. Only then move on to large-scale implementations.

Rule 7:

The key components of e-government are digital databases, a secure data exchange platform, digital identity, an online services portal and a metadata management system with a services catalogue. These are complemented by digital document management systems in ministries and other institutions and by sectoral online solutions. The primary databases are the civil registry (population registry), the real estate registry and the business registry.

Rule 8:

Upon commencing implementation of e-government, sustainable financing mechanisms should be planned. This involves the national budget. The costs of running e-government projects cannot be financed completely by private investment. Budgeting for e-government at the national level also promotes its implementation and coordination.

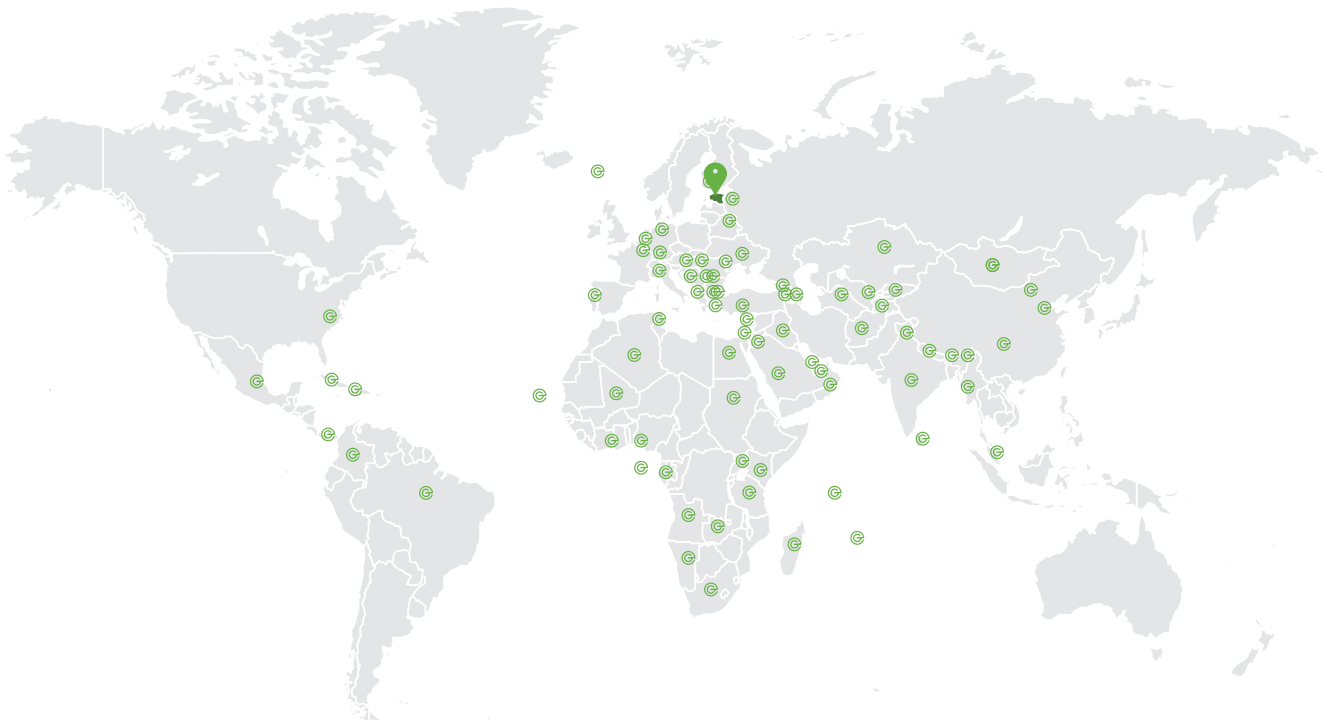
Rule 9:

A supporting legal framework should be developed as an integral part of e-government implementation. Legal issues surrounding personal data protection, privacy, data security and other matters should be resolved by the time ICT systems are launched in the government.

Rule 10:

Cyber security measures should be implemented across the government together with measures for protecting vital infrastructures. Successful cyber security comes not only from technology and responsible ICT workers, but from all government officials' observing proper digital and non-digital protocol.

Let's turn e-governance on!
Everywhere.



eGA 15 YEARS Empowering e-governance around the world

e-Governance Academy Head Office
Rotermanni 8, 10111 Tallinn, Estonia
+372 663 1500 | info@ega.ee | ega.ee
Follow us on Facebook and Twitter: egovacademy