E-government Ecosystem

Hannes Astok

Senior Expert, Executive Director

E-governance Academy, Estonia

What is digitalisation?

What does digitalisation of society mean? Why does it matter? What is e-government?

European Commission

Key aspects of digitalisation and e-government

- Not primarily a technology question: Change management
- The new technologies should not be used to just do the same thing (not to use computers as typewriters!)
- There should not be too much specialised legislation on digital issues, to avoid creating parallel systems
- Cooperation between the public and private sectors is essential
- The need for a citizen-centric approach: questions of trust, the perception of people

Digitalisation for whom?

- IT is a science at the service of man, it must not infringe on human identity, the private life of the individual, human rights, individual or collective freedoms.

Law No. 2009-09 on the protection of personal data in the Republic of Benin

Digitalisation for whom?

- Digital solutions are not only or primarily for the richest, most developed countries but many innovative solutions can be used to leap-frog development stages and to address specific challenges
- Examples:
  - Estonia paperless government since 2000 (9 years after re-independence)
  - Mobile banking system M-Pesa, Kenya
  - Online court hearings and/or giving evidence or making depositions in the Caribbean Community (CARICOM) Court of Justice

Key values of e-government

Key values of e-government

- Citizen centricity
- Once only principle
- Privacy and personal data protection
- Respect of human rights online and offline
- Inclusiveness
- Single digital market approach

Citizen centricity

- Putting the citizen at **the center of governance**
- Involving citizens in the design, delivery and review of public services
- When governments deliver services based on the needs of the citizens they serve, they can **increase public satisfaction** and **reduce costs**
- Technology can assist processes simplification and redesign
- ICT is a good tool for it, but not the solution

Once only principle

- Citizens and businesses should not be asked to **provide the same data more than once** in contact with public administration
- Public administration bodies take actions to **internally share and reuse data** – even across borders – always in respect of data protection regulations and other constraints
- The legal and practical question of who/which authority that should be granted access to data is to be seen **separately** from the question of possible technical access through mechanisms of interoperability

Privacy and personal data protection

- Privacy and personal data protection are essential for trust between the citizens and government and for people´s perception of the digital society
- The General Data Protection Regulation (GDPR) has importance also outside of Europe (due to its effect on data of EU citizens and as it is used as a model)
- The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU and ensuring adequate protection also outside the EU

GDPR basic principles

1. **The Principles of Lawfulness, Fairness, and Transparency**: The personal data needs to be processed in a way that is lawful to the subject
2. **The Principle of Purpose Limitation**: The data processors can only use the data for the objectives they have explicitly described and justified
3. **The Principle of Data Minimization**: The information that is required has to be relevant for its purpose and limited to what is necessary

GDPR basic principles (2)

4. **The Principle of Trueness, Accuracy**: If some of the data is inaccurate, it should be removed or rectified
5. **The Principle of Storage Limitation**: Data is kept in a form which permits identification of persons for no longer than is necessary for the purposes for which the personal data is processed
6. **The Principle of Integrity and Confidentiality**: This principle stands for taking all required measures to ensure that all personal data is protected

Data protection legislation globally

- Many countries have recently passed data protection legislation, inspired to a large extent by the GDPR (but with some local and regional differences)
- A few examples among many:
  - Thailand (adopted 2019, in force 2022)
  - Brazil (adopted 2018, in force 2020)
  - Kenya (adopted & in force 2019)

Respect of human rights online and offline

The same human rights apply online and offline, but measures for protection may look different

Digital tools allow for effective **access to information**

Digital tools can be used to **enhance rights-protection and empower people** to know and claim their rights

> Example: The digital footprint left in Estonia - that people can easily see- when authorities access personal data

Human Rights Challenges

- Freedom of expression vs. hate speech
- Correct vs. misleading information
- Real vs. fake news
- Impact to elections
- Democracy development issues
- Digital divide, discrimination (lack of access to digital tools)

Inclusiveness

Includes various categories of inclusiveness:

- Availability
- Affordability
- Relevance
- Readiness
- Gender issues

The Inclusive Internet Index 2020

MENTIMETER

E-government enablers

Analogue and digital elements

European Commission

Before going digital…

…we need to ask, is there available basic infrastructure

- Electricity
- Connectivity
- E-governance development can start alongside infrastructure development
- Connectivity problems can be solved with regulatory measures to stimulate competition and remove unnecessary taxes

Analog and digital elements of e-government

Analog elements

- Legislation & regulations
- Sustainable organization
- Fiscal framework
- Change management
- Political will
- Digital skills

Digital elements

- Digital databases
- Interoperability
- Digital Identity
- Services portal
- Cyber security
- Document exchange
- Sectoral solutions

Source: Digital Dividends. World Bank report 2016

Key digital elements

- Digital databases
- Interoperability solution – secure data exchange
- Digital identity
- Digital documents exchange
- Services portal

Those elements are shared (or platform) services,

to be shared across the government

Digital data

European Commission

138252

Principles of digital databases development

- Unique numeric identifiers for citizens, businesses, real estate, land parcels, etc.
- Unique numeric identifiers are used across the government for all transactions
- Once only. Citizens never have to provide the same information twice
- No duplicated data in the databases
- Databases become the single source of truth

Principles of digital databases development (2)

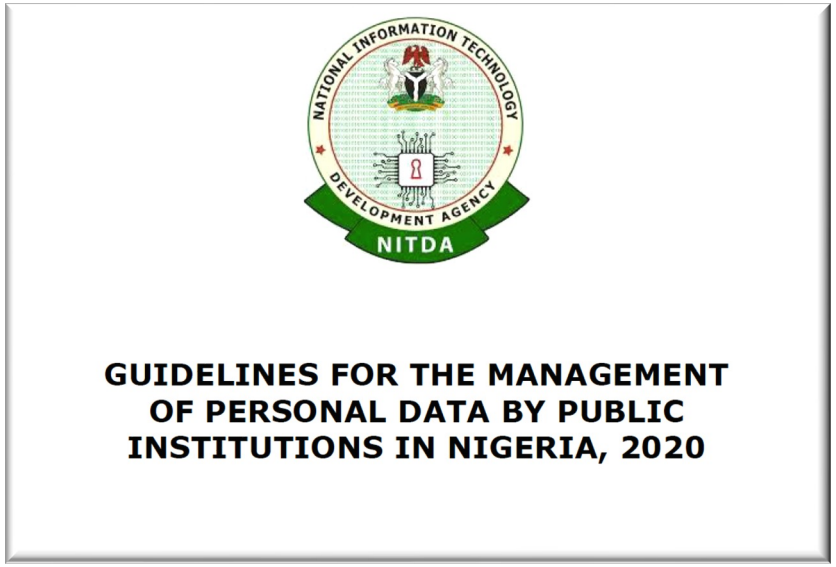
- Central registry of databases metadata and online services, “database of databases”
- Clear data ownership
  - Data is owned by the citizen
  - Databases are owned by the institution that creates and manages them
- Each authority is responsible for own database quality

How to make data digital?

- New data: immediate digital capture
- Historical data digitalisation:
  - Massive digitalisation year by year
  - By request

Nigeria

- Nigeria has plans to migrate all government paper activities to paperless by 2030.
- Since May 2020, the National Information Technology Development Agency (NITDA) requires all Public Institutions holding or processing personal data to securely digitise all personal databases
- Budget for digitisation increased manifold in 2021 compared with previous years

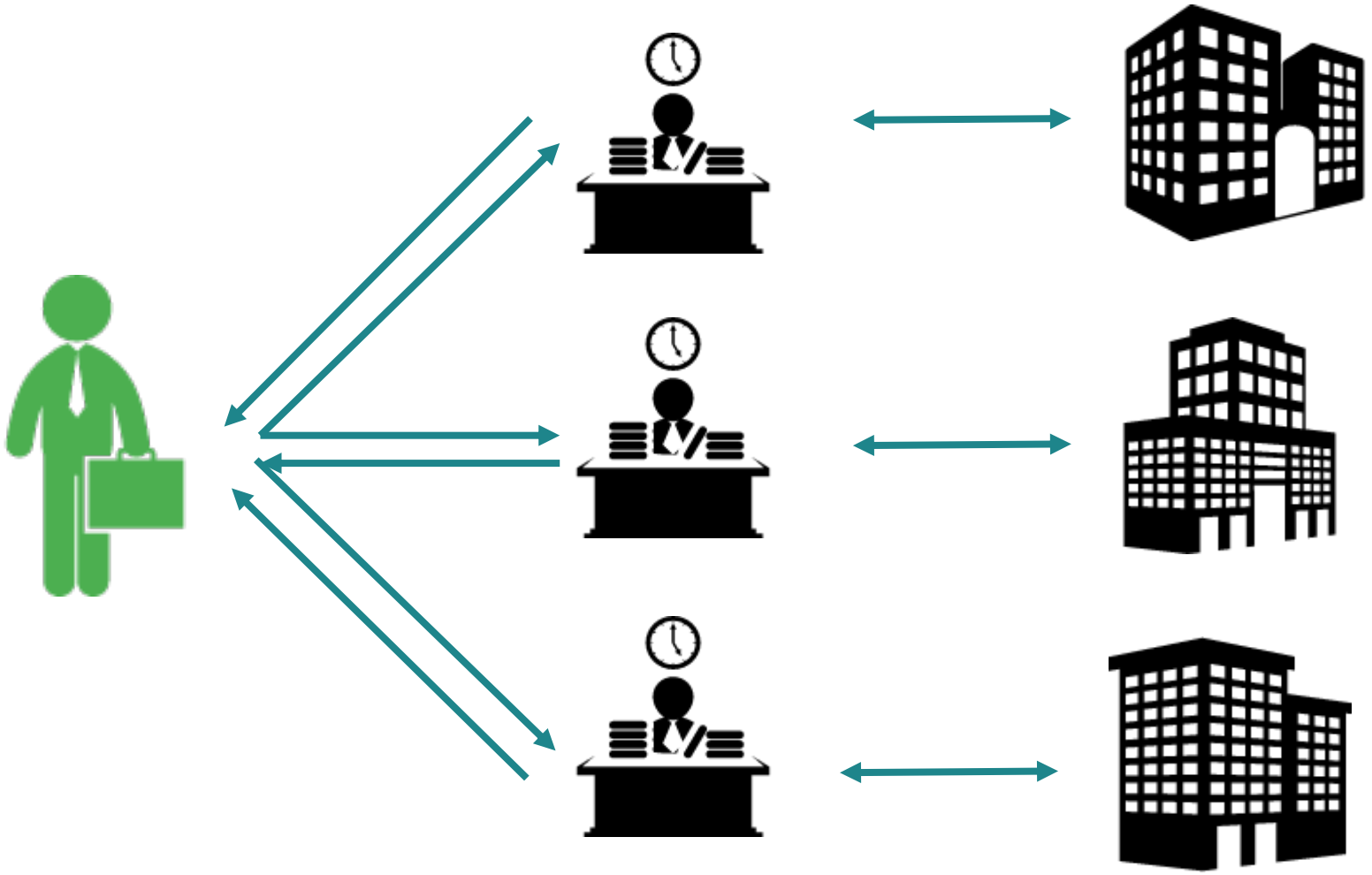


European Commission

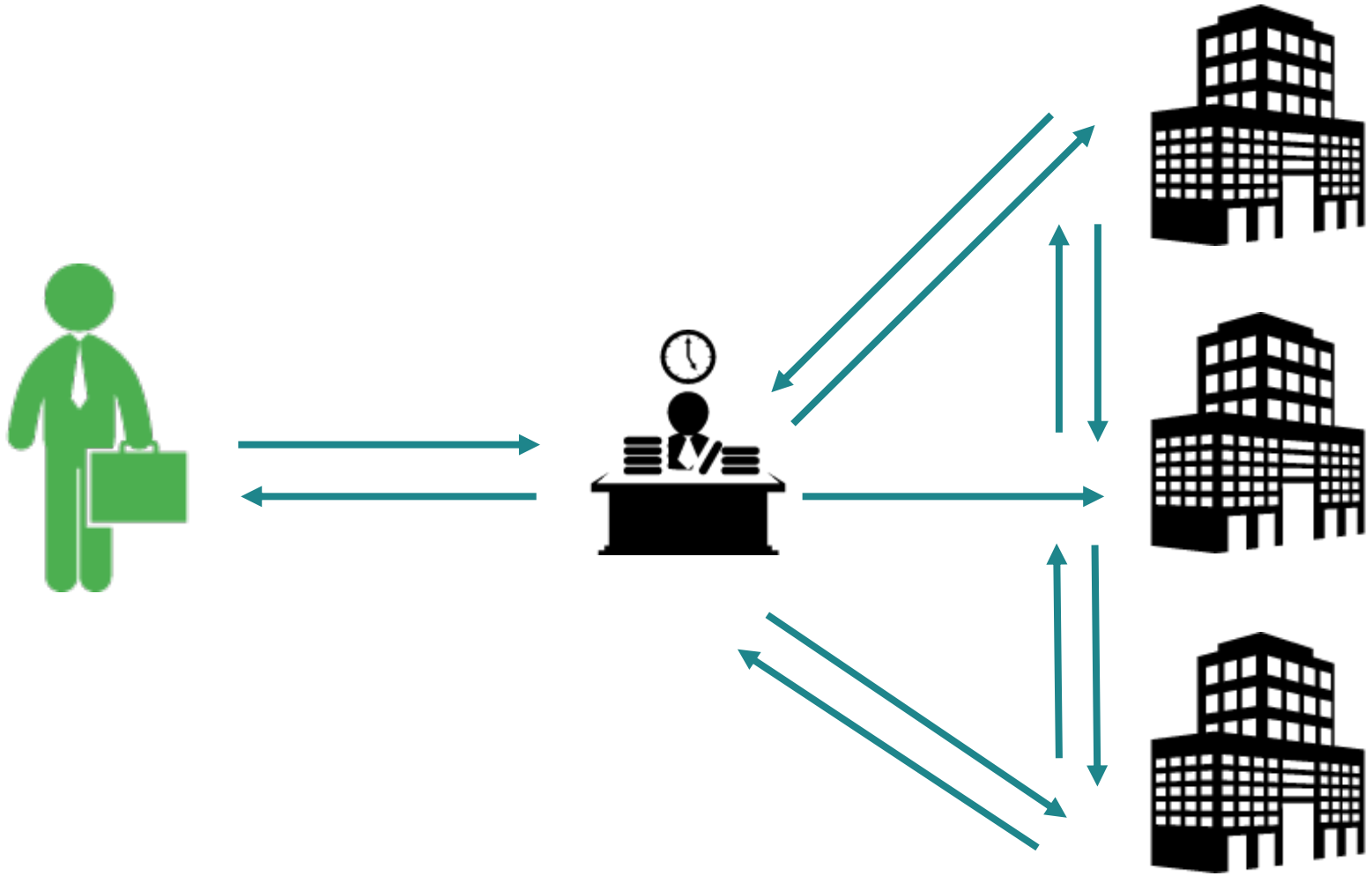
Interoperability

European Commission

Traditional public service delivery

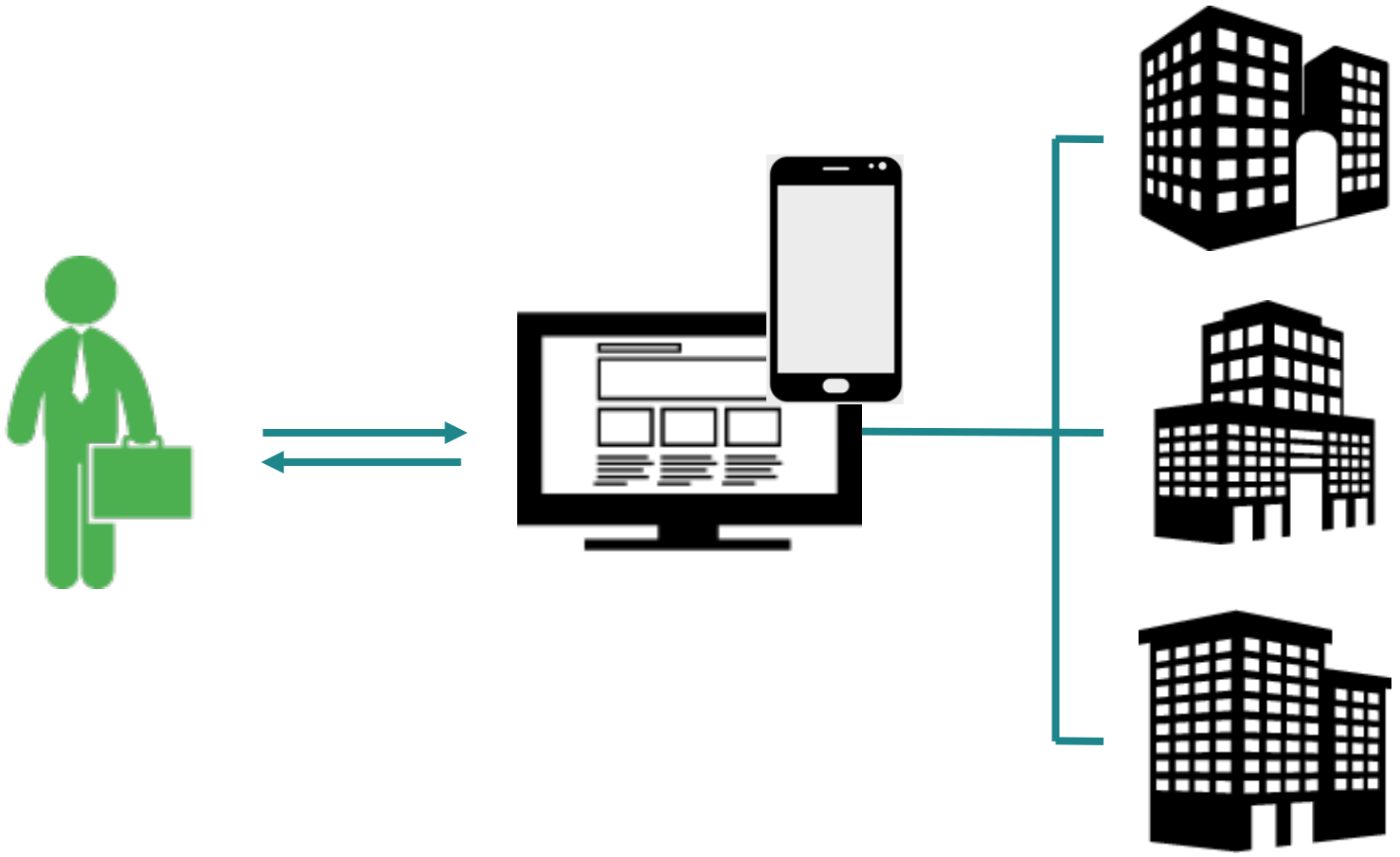


One-stop-shop

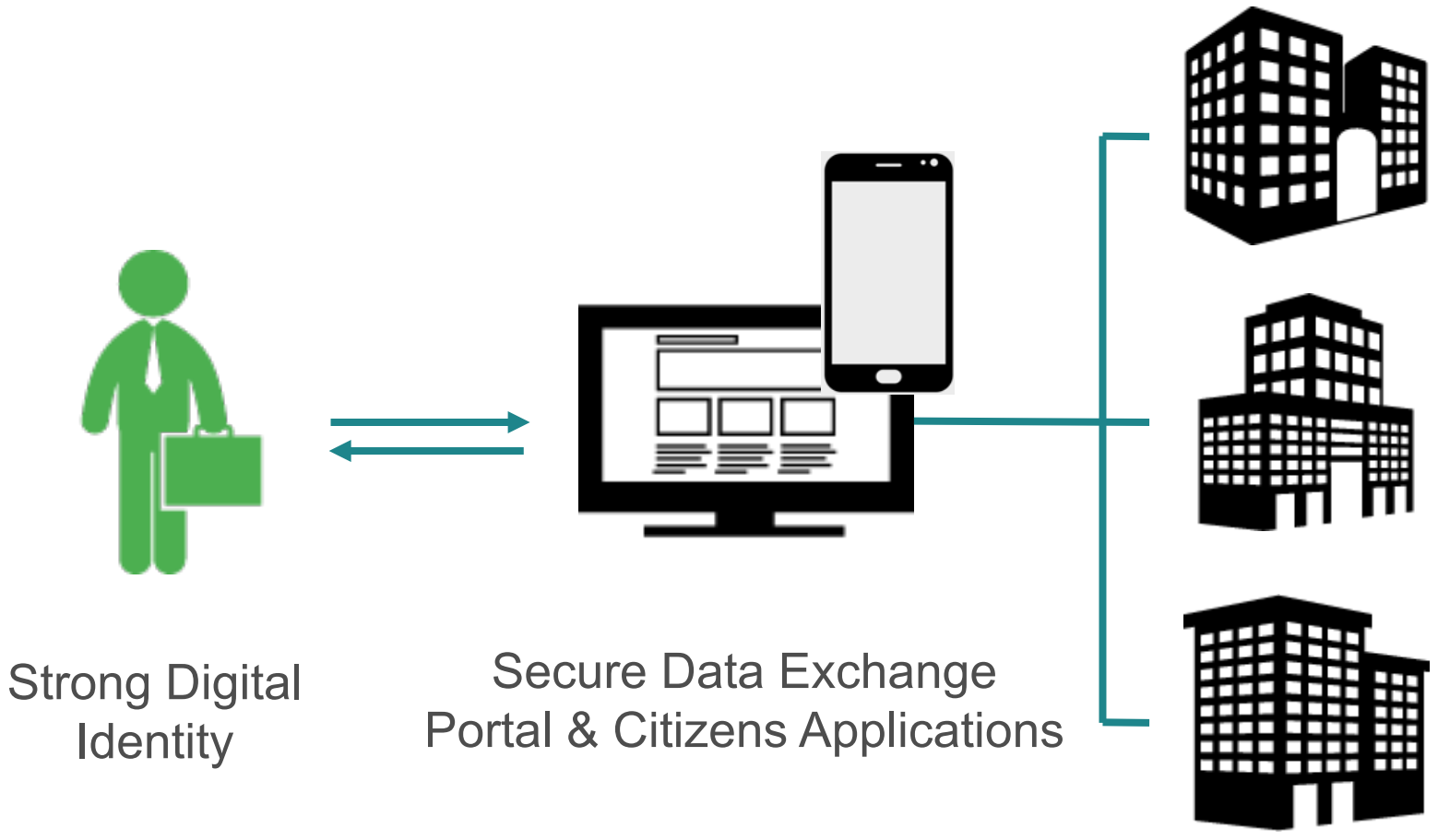


European Commission

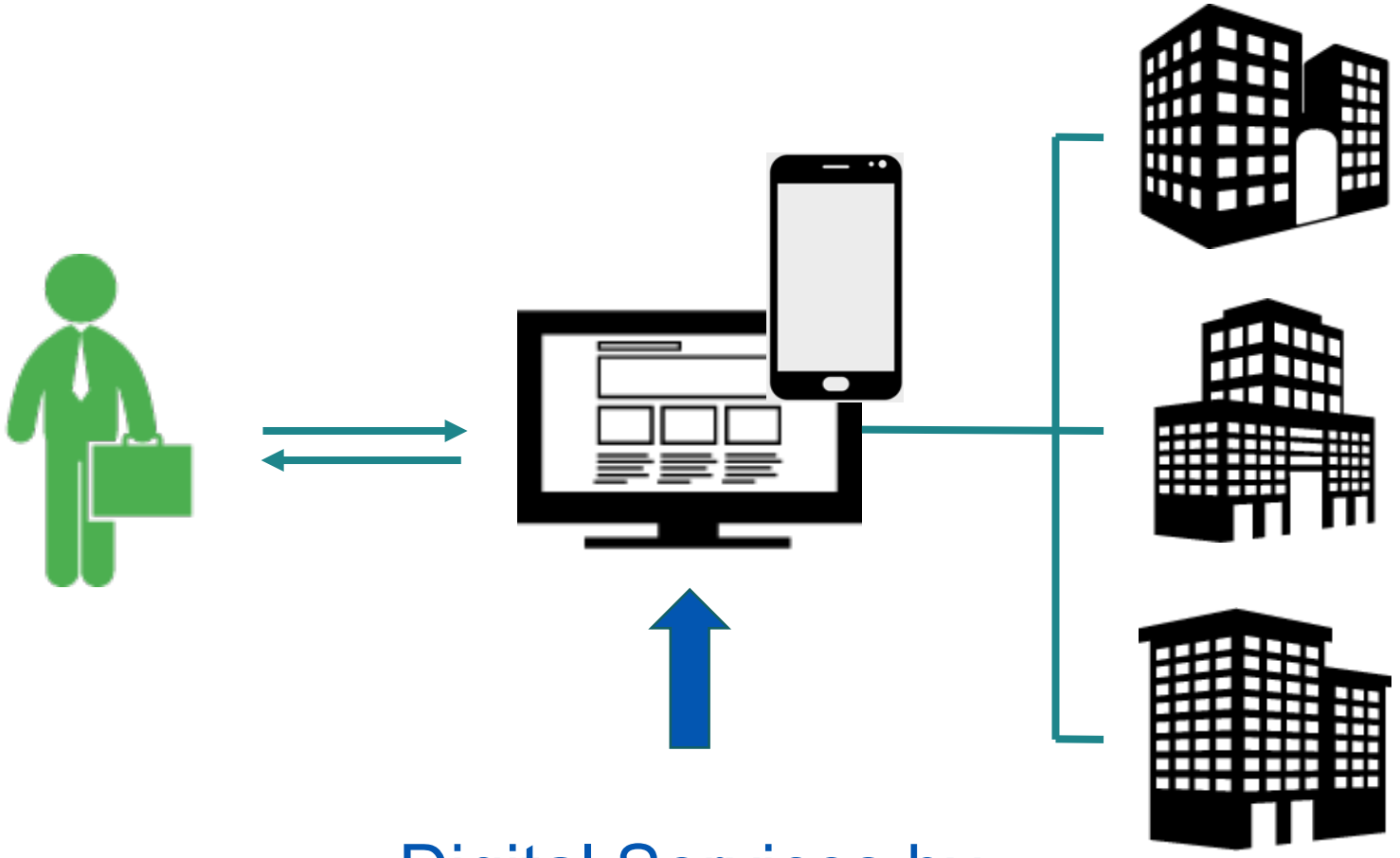
Self service



Self service enablers



Digital services by service owners



Digital Services by
Ministries I Agencies I Municipalities

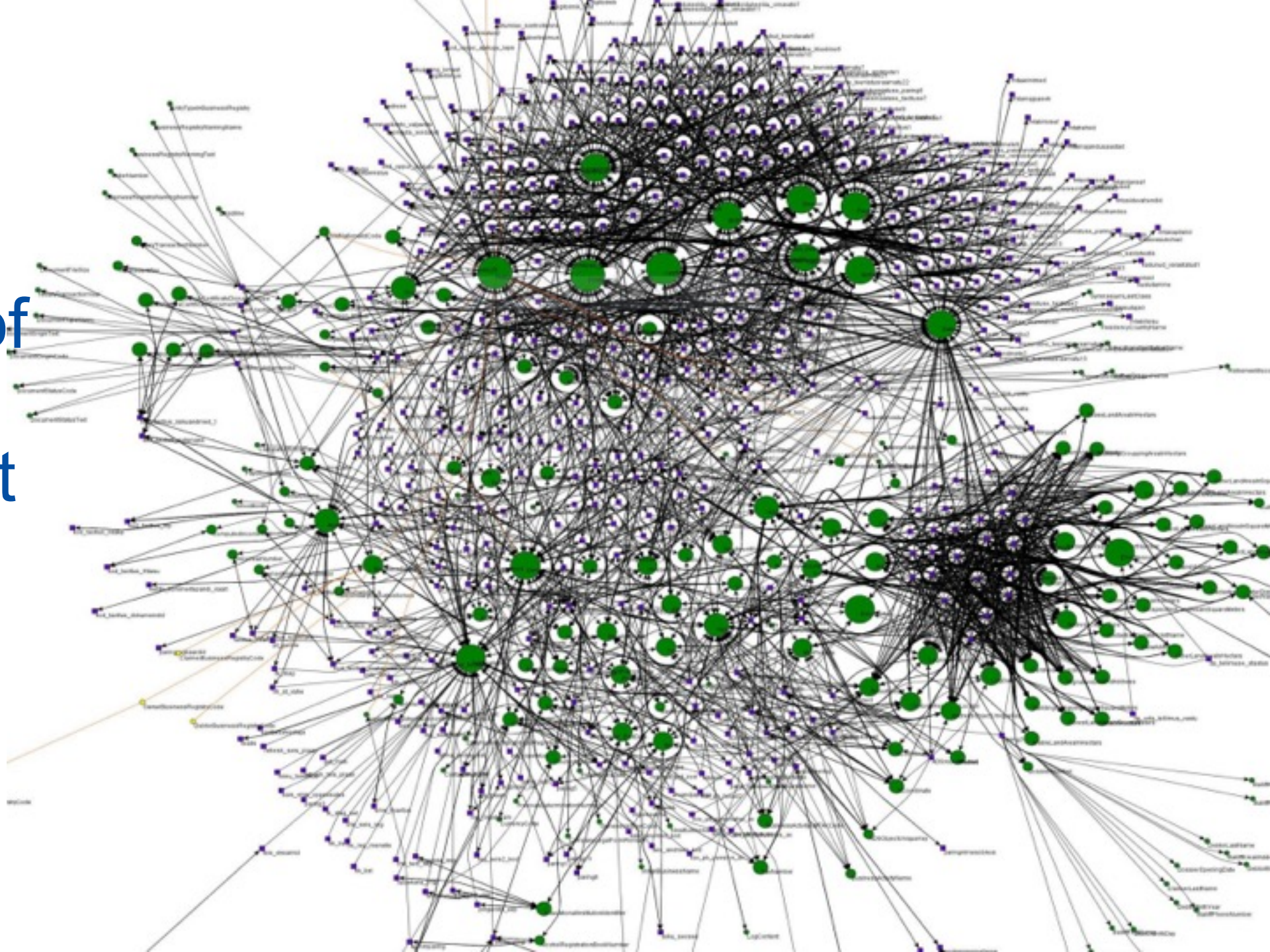
European Commission

Online versus offline: applying for certificate

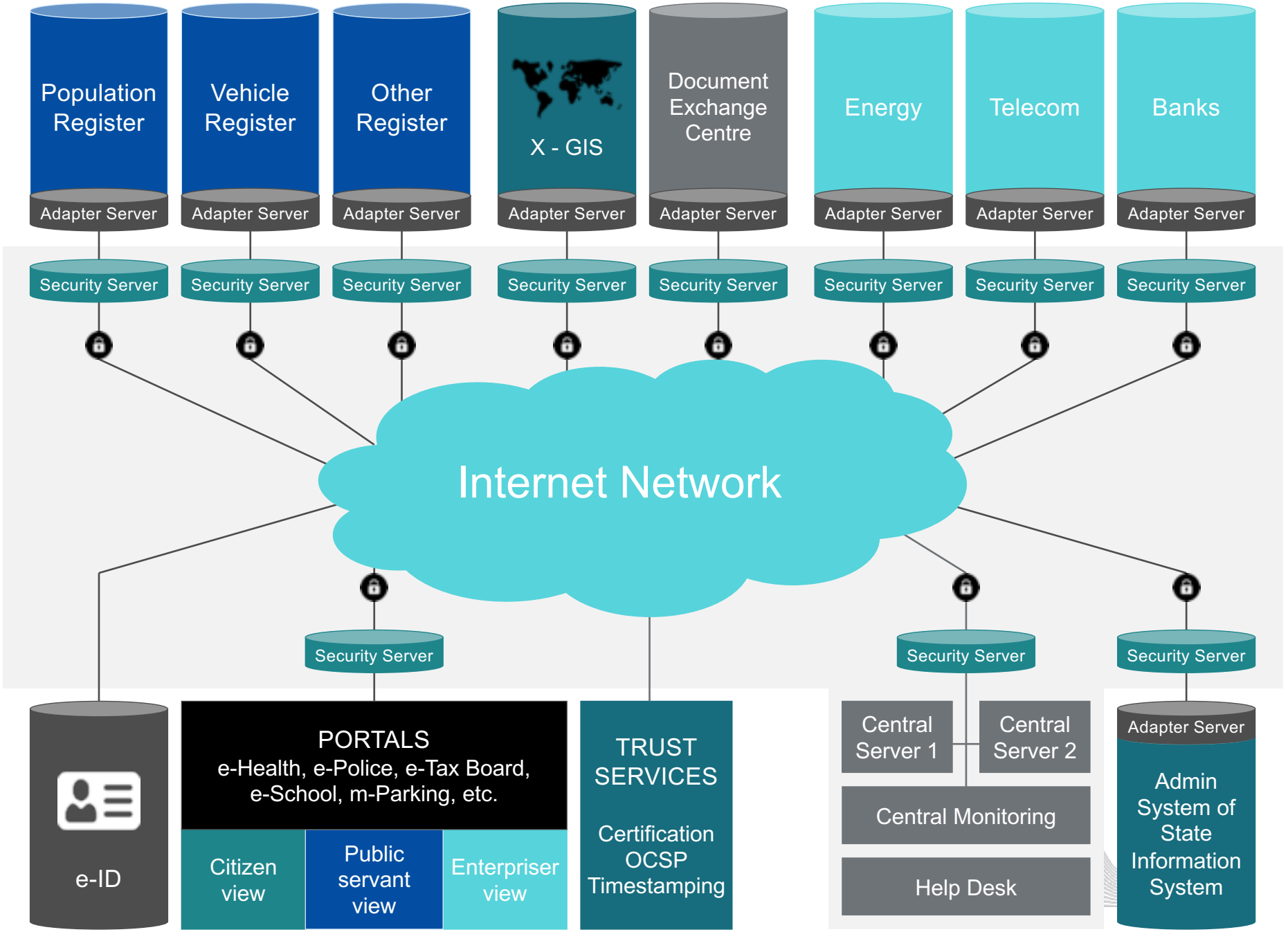
Activity	Time offline (hours)	Time online (hours)	Win
SUBMISSION			
Travel to the government office	4	0	
Filling the application	0,5	0,5	
Waiting in line to submit the application	3	0	
Submitting the application	1	0	
Travel back home	4	0	
PICK-UP			
Travel to the government office	4	0	
Waiting in line to pick-up the certificate	3	0	
Pick-up of the certificate	0,5	0	
Travel back home	4	0	
TOTAL	**24**	**0,5**	**23,5**

Actual data exchange of in any government

Non-organized model



Organized data exchange model X-road Estonia (Namibia, Benin)



Sample: Before paying out pensions in Estonia

500,000 pension and subsidy payments/month

Request: Are they alive? (sending ID-numbers)

Pension Authority

Automated response: Those 980 passed away (response as ID numbers)

Time-stamped+digitally signed

Civic Registry

Interoperability Solution

European Commission

Benefits

- No need to collect and verify similar datasets by every institution
- Single sources of truth are easily accessible
- Easy to develop services
- Every transaction is verified and timestamped
- Transactions with legal value

Digital identity and digital signature

European Commission

Unique Identifiers

- Allows **unambiguously identify** individuals, businesses, land parcels, buildings, vehicles
- Should be unique and machine readable
- May contain numbers and/or letters, may be composed from content elements (like date of birth) or be serial or random
- Examples of challenges:
  - Namibia: People with several different names in different databases (legacy from apartheid era)
  - Benin: People whose births have never been registered in any form

Why do we need strong digital identity?

- Connects physical identity and digital identity
- If provided and trusted by the government, easy to use for businesses also
- Should be based on proper population management system, not as a stand-alone solution
- Should be suitable both for government and business transactions (banking, etc.).
- Also, future cross-border transactions should be considered.

Efficiency


Digital signatures save 20 minutes per transaction
World Bank World Development Report 2016

Cost-profit calculators

- **Up to today Moldovan citizens have provided 75 million digital signatures**
- People and companies have saved more than 150 million € (2 € per signature)

Actual savings may be greater:

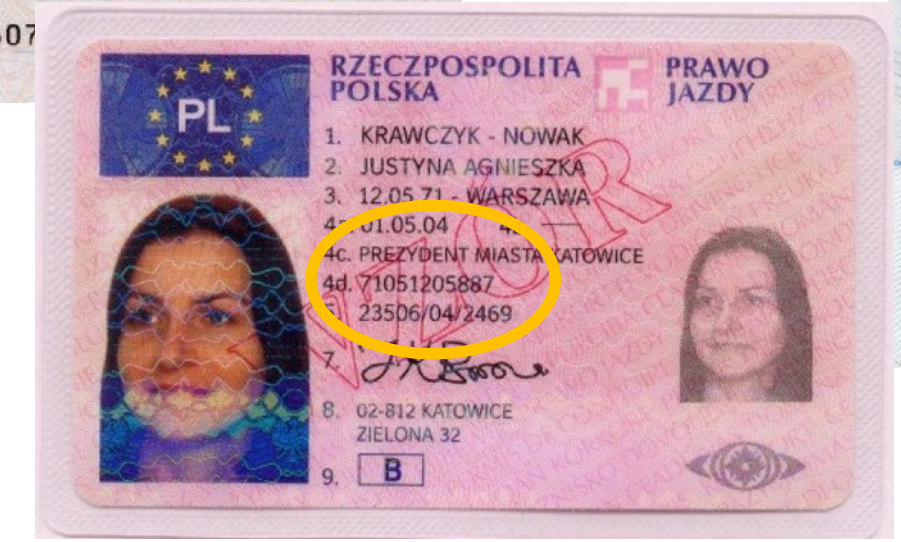
http://eturundus.eu/digital-signature/

http://eturundus.eu/digital-document/

Source: Moldovan E-Government Agency

European Commission

Unique ID Number in documents (Poland)



European Commission

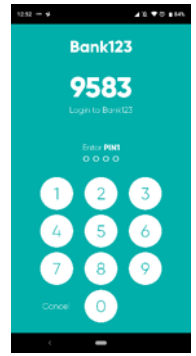
Unique ID Number documents (Bangladesh)

European Commission

Digital identity carriers

Typical carriers of the certificates are:

- eID cards
- Flash drives
- Mobile phone SIM cards
- Smart phone applications



European Commission

In the device are usually stored two certificates

- 1st certificate for identification
- 2nd certificate for digital signature

European Commission

Where to use digital identity?

- Usually, there is a need to sign the applications for public services
- The same need is the need to sign contracts and other documents

Typical scenario:

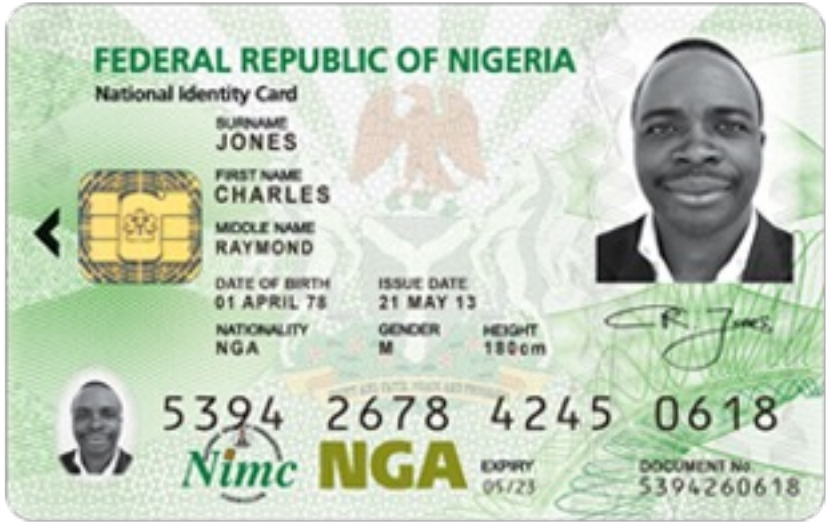
- You need to **sign in** to the application –using 1st certificate for identification
- You need **to sign the application or document**: using 2nd certificate for digital signature

What is eIDAS framework

- **eIDAS** (Electronic Identification, Authentication and Trust Services) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market (2014)
- Makes available **cross-border recognition of digital identity.**
- Member states are required to create a common framework that will recognize eIDs from other member states and ensure its authenticity and security. That makes it easy for users to conduct business across borders.
- eIDAS provides a clear and accessible list of trusted services that may be used within the centralised signing framework. That allows security stakeholders the ability to engage in dialogue about the best technologies and tools for securing digital signatures.

Nigeria national ID card: 5 functions

- From 2014
- Over 30 M cards issued as end 2019



European Commission

Nigeria national ID card: 5 functions

1. National identity card
2. Travel document based on ICAO standards
3. Electronic ID - offers strong authentication and digital signature.
4. Biometric eID - The card contains 10 fingerprints captured during the registration procedure.
5. Payment card - The payment application turns the Nigerian national ID card into a tool for payments or can be used at ATMs or for transfers.

In a second phase, complementary applications such as a drivers' license or e-services including eVoting, eHealth or eTransport are to be implemented.

Portal and citizen applications

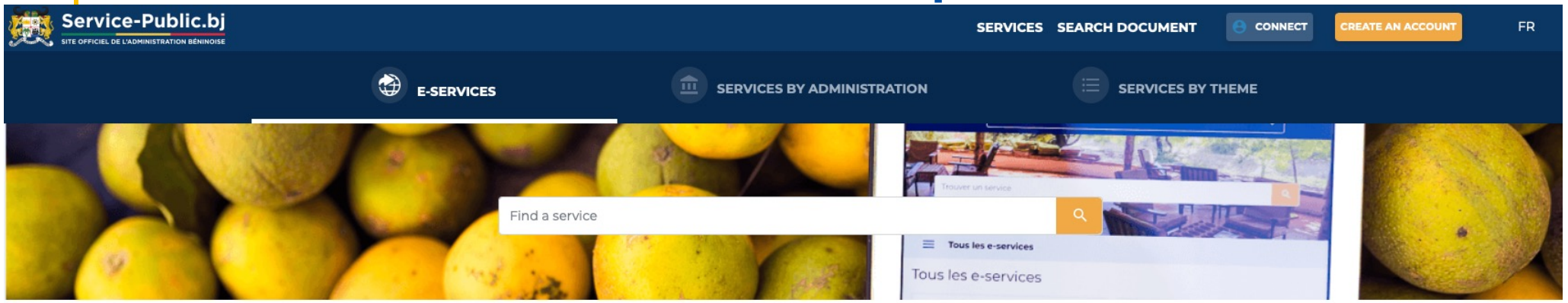
The practical use of e-government

European Commission

Portal & citizens applications

- The portal technically assembles digital services
- The web and mobile applications are visible front-end of the services
- They cannot function without back-end, i.e., digital databases, secure data exchange, digital identity, etc.
- Also, online payments gateway is usually embedded in the portal to ensure necessary payments during the transaction

Benin national service portal



- All e-services
- Affaire/Entreprise
- Affaires sociales
- Affaires étrangères/Diplomatie
- Aviation
- Cadre de vie
- Commerce
- Communication
- Culture et Tourisme
- Digitalisation
- Domaine et foncier
- Education/Enseignement
- Energie

All e-services

Attestation de confirmation cadastrale

Attestation de confirmation cadastrale

Show details

Apply

Attestation de jouissance de droits à une pension de retraite

Pièce attestant que l'intéressé jouit de sa pension de retraite au FNRB

Show details

Apply

Attestation de prise en charge pour les agents admis à la retraite

Pièce attestant que l'intéressé jouit de sa pension de retraite sur le FNRB

Show details

Apply

Attestation d'affiliation au FNRB

Pièce attestant que l'intéressé cotise au FNRB

Show details

Autorisation d'exploitation de réseau filaire ou optique

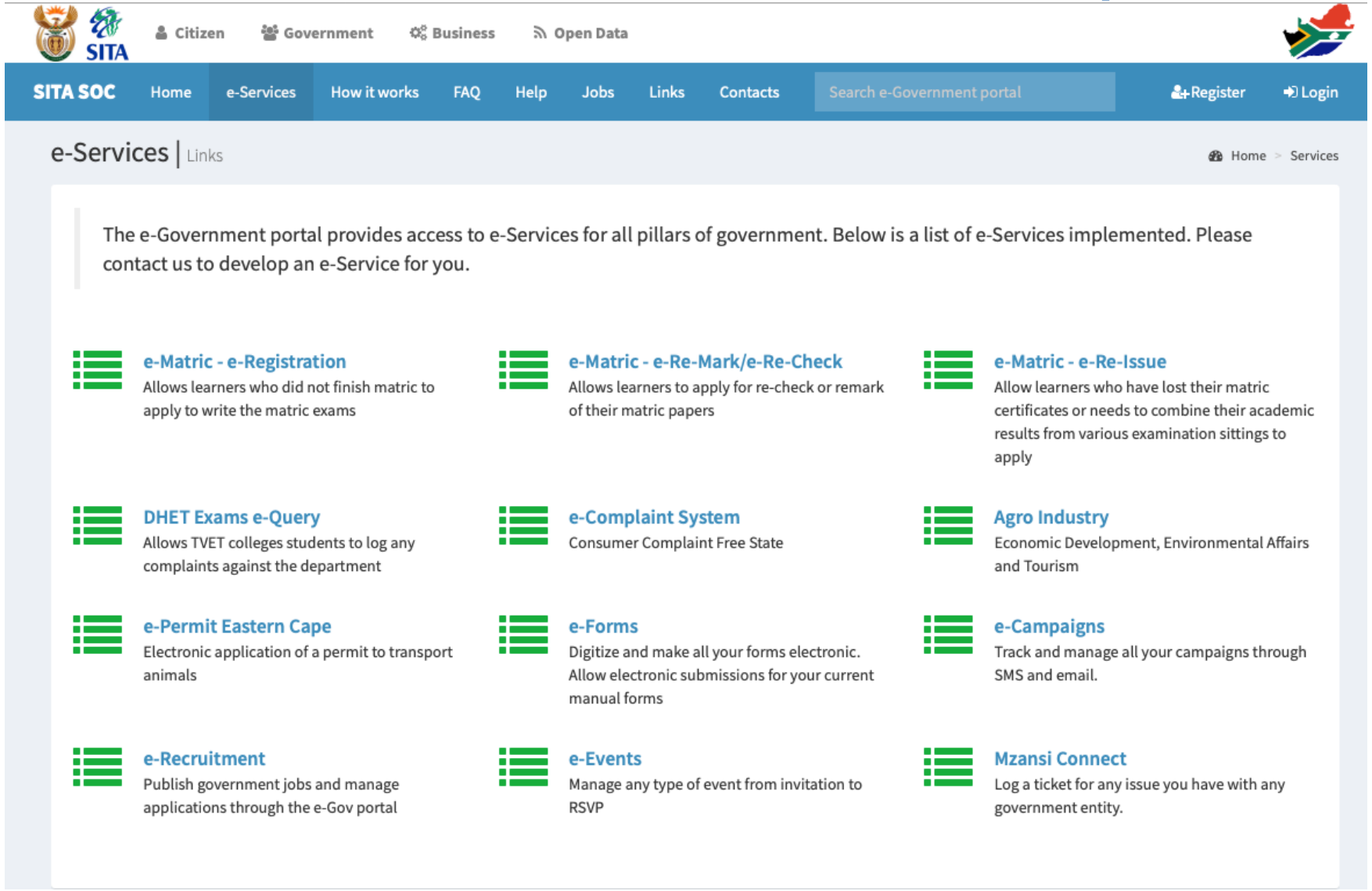
Show details

Autorisation d'établissement de Réseau RMU ou 3RP

Show details

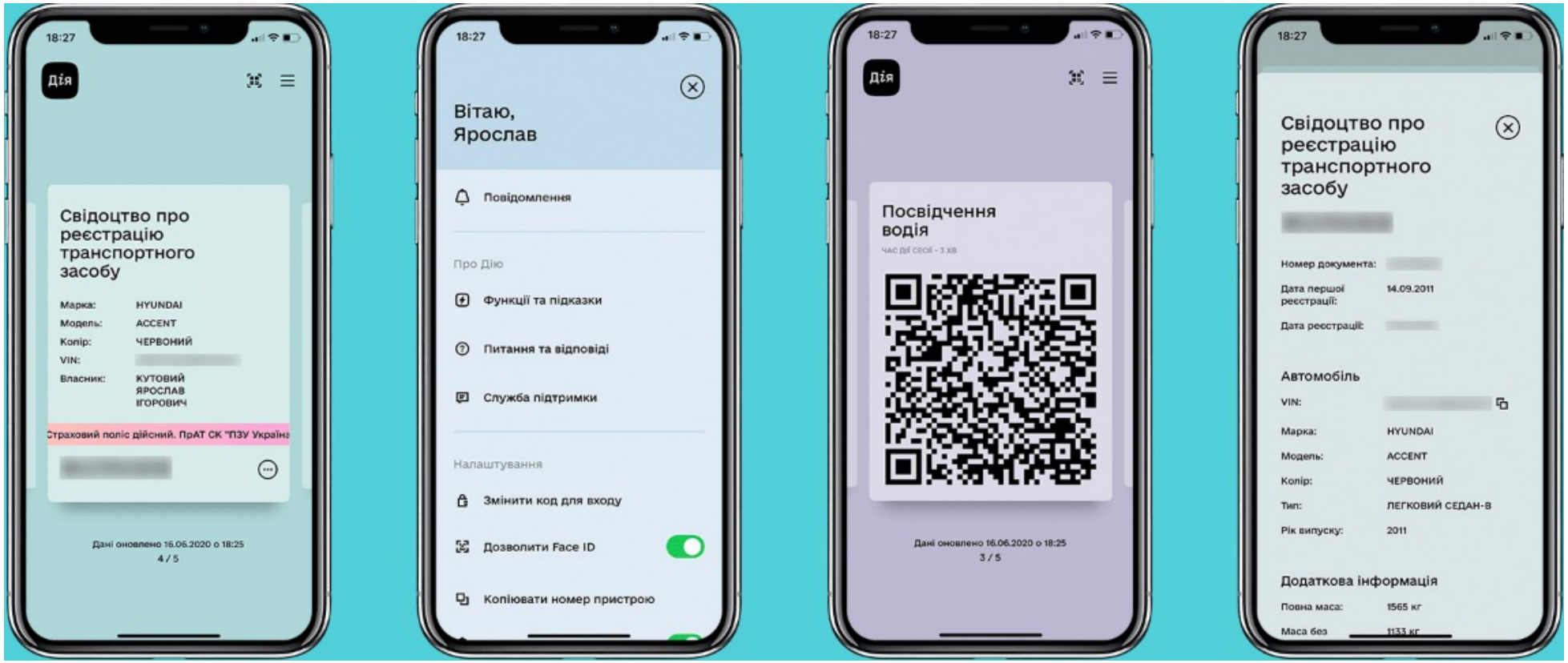
European Commission

South Africa national service portal



European Commission

Ukraine government mobile app DIIA



European Commission

Analogue enablers

Legislation, organisation, financing

European Commission

Key analogue elements

- Legislation and regulations
- Supportive organisation
- Sustainable budgeting
- Change management
- Political will
- Digital skills

Legislation and regulation

- There should not be too many specialised laws
- Laws should be technology neutral – focus on aims and not (mainly) methods
- Technical and legal possibilities for data exchange must be treated as different issues – but technology can help to protect rights
- The legal issues are largely horizontal
  - Digital Identity, validity of digital signatures
  - Data protection
- Involve lawyers in early stage of e-government reform!

Supportive organisation

- **Horizontal coordination** of the e-government activities, not concentration of all activities to one government entity
- The coordination unit should be close to the power (President or Prime Minister Office) to be able to push for change
- Clear roles and responsibilities with resources for all stakeholders across the government
- Engagement of the stakeholders at all levels
- Motivated staff

Sustainable budgeting: typical costs for e-government

Investment costs

Building of data centers

Building of the networks

Purchase of hardware

Purchase of other equipment (office equipment, cars, etc.)

Purchase or development of information systems;

Purchase of software licenses.

Running costs

Staff costs

Rent of equipment and rooms

Electricity, heating, cooling

Rent of networks, computing and storage capacity

Annual software licenses, support and maintenance, upgrades.

Financing models

- Shared services: financed centrally from national budget, no fees for government institutions or for customers
- Each ministry, agency, municipality responsible for own services financing
- National funds for development of priority solutions (investments)
- Daily operations budgeted as operational expenses/running costs in the government entities

How much does it cost?

- EU MS practice shows that annually 1,5-2% of total government budget should go to e-government spending to be successful
- Life cycle for hardware is about 5 years and for software for complex ICT solutions maximum 12 years.
- When procuring, look at the total cost of ownership (TCO).
- TCO consists all costs during the life cycle. The trap may be in the annual licenses, support and maintenance fees on the top of the initial investment.
- In the donor financed projects, governments tends to forget about the later running costs (licenses, support and maintenance, additional developments, etc.). It should be clear who pays those costs.

Change management

The role of information technologies in public administration:

- To support data sharing and process re-engineering
- e-governance is about reforming and modernising Public Administration with ICT tools, not limited to the computerisation of government offices
- e-governance is a comprehensive set of organisational, regulative and technological measures, not just computer software and hardware

Change management

Simplification of the business processes in the government and in the related services

Bottleneck is usually between the computer and chair

Motivation of the officials to take up new solutions

Fear to lose the job: no massive layoffs as online services takeup will take years

Change management and political will

- To gain results and impact, the government must have a vision and a plan
- This needs to be accompanied by leadership, organisation and resources
- There must be political will to sustain the changes: Buy-in of the political leaders is one of the critical success factors
- This will provide resources, necessary legislative changes and support for change management

Cybersecurity

A key consideration for all digital solutions

European Commission

Cybersecurity: What is it?

- *The desired end state in which the cyber domain is reliable and in which its functioning is ensured.* Source: Finland's Cyber Security Strategy Government Resolution (24 Jan 2013)
- *The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them*. Source: New Zealand's Cyber Security Strategy (June 2011)

Cyber security

- Complex issue: mixture of digital and analog elements
- Roles and responsibilities in the government
- Technical measures
- Behavior of officials
- Awareness of the citizens

Critical Infrastructure Protection

- Critical infrastructure identification and protection and Security of Network and Information Systems: an “all-hazards approach”, for relevant networks in fields like energy and transport
- Importance of designation of what is critical infrastructure, definitions, risk-assessment tools, designating responsible persons
- Computer Emergency Response Teams, Computer Security Incident Response Teams and similar functions
- “Regular” regulatory (ICT, energy etc.) law is also an instrument for (critical) infrastructure protection

Cybersecurity: Cybercrime
The Budapest Convention

- Convention on Cyber Crime (23 November 2001, Council of Europe – open to all states)
- In force 1 July 2004
- 65 parties (Europe, USA, Japan, Senegal, Sri Lanka, Australia, etc.)
- Plus Protocol on Xenophobia and Racism

Future of online governance

European Commission

The future government is

Proactive

Online

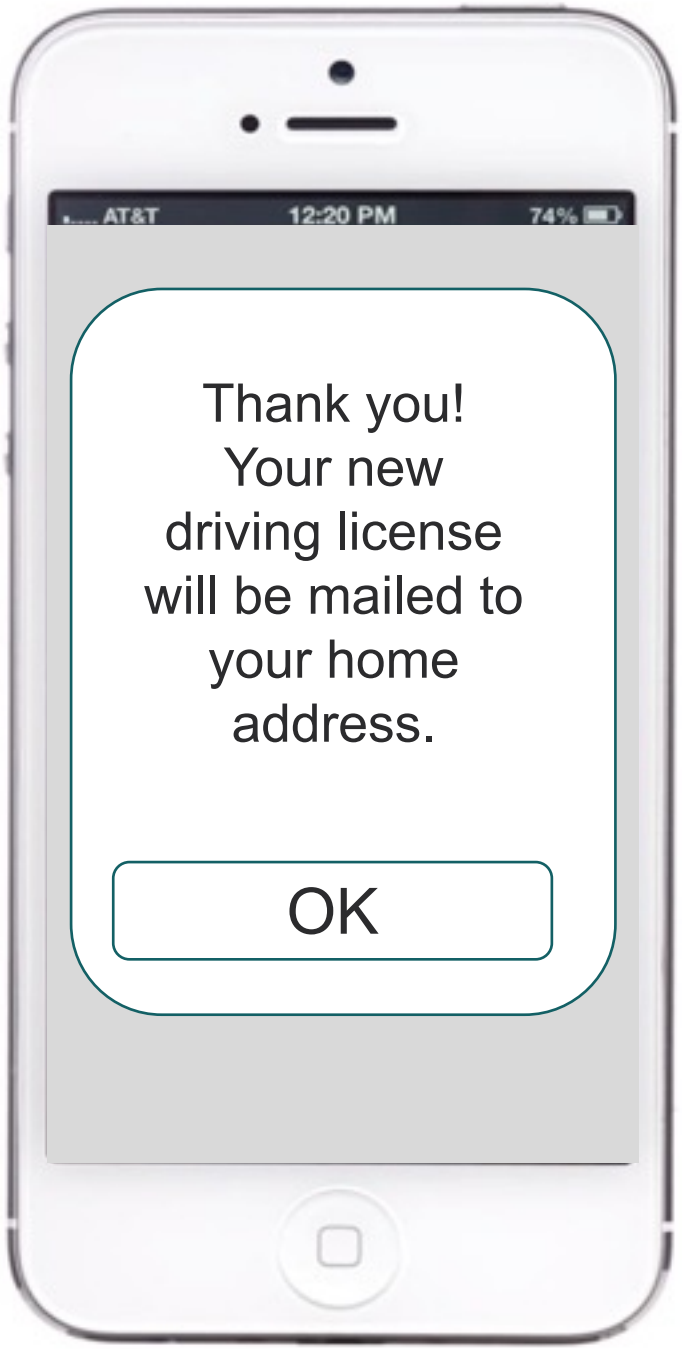
24/7

Intuitive

European Commission


AT&T
12:20 PM
74%
Government app


AT&T
12:20 PM
74%
Mr. John Smith, your driving license will expire soon. Can we mail you the new one? Your Government
Yes
No


AT&T
12:20 PM
74%
Thank you!
Your new
driving license
will be mailed to
your home
address.
OK

Thank you!

Hannes.Astok@ega.ee
Mobile/Whatsapp +3725091366

Slides pictograms: E-governance Academy www.ega.ee and Freepik; Slides 37-39 photos Hannes Astok

European Commission