KYRGYZ DIGITAL CODE

IDEAS, APPROACHES, STRUCTURE

Codified Legislation

Law on Electronic Governance, 2017

Law on Electronic Signatures, 2017

Law on Biometric Registration of Citizens, 2014

Law on Personal Information, 2008

Law on Electrical and Postal Communications, 1998

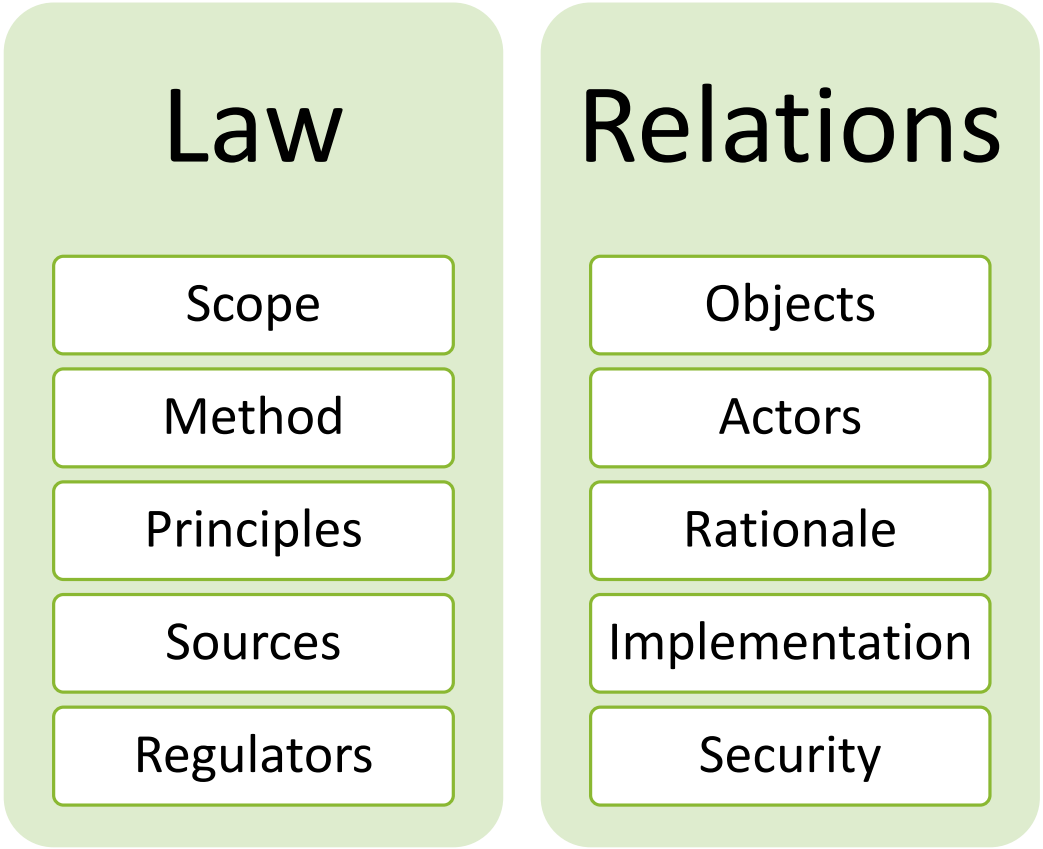
The Code place in regulating the digital environment

Public relations in digital data processing, including through the Internet, create cyberspace as a single digital environment without territorial boundaries. Citizens, legal entities, the Kyrgyz Republic, as an independent subject of legal relations in the digital environment, create communities in the digital environment (digital communities) and participate in them, and therefore have the right to participate in determining the rules for these communities.

The number of Internet users in the KR - 5.4 million (less than 0.1% of the number of users in the world) - does not allow to insist on the concept of sovereignty in cyberspace, promoted by large states. But this does not deprive Kyrgyzstan of the right to propose its own approaches to regulation and to comply with the rules it sets for itself.

The Code was developed as a digital constitution of Kyrgyzstan and is based on an understanding of cyberspace as a global, cross-border and very complex environment, where everyone should have a place and where everyone should participate in determining the rules, based on which the digital environment functions and develops

Regulatory structure



The Code's general part contains the basic normative provisions, which are characterized by a high degree of generalization, stability and lay down the legal basis for the use (application) of the norms of the special part.

The provisions of the General Part of the Code lay the foundations of digital law as a new branch of legislation and define the elements of those social relations that are regulated by the Code

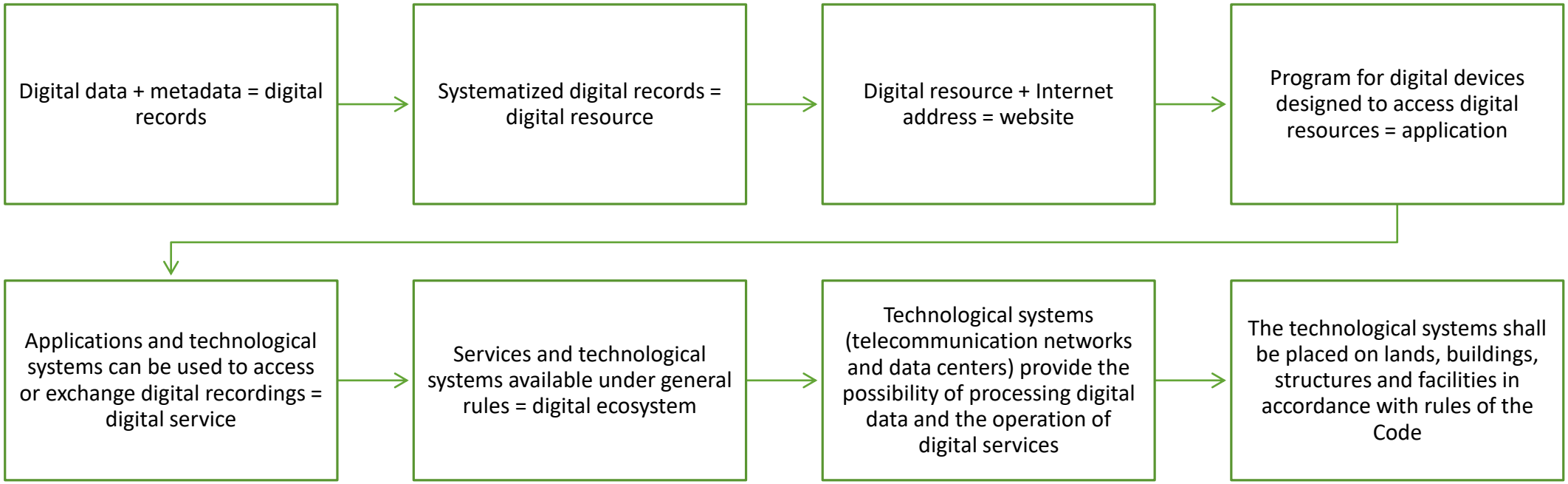
Scope and levels of regulation

Data	• Digital data and records • Digital resources • Sites and mobile applications
Services	• Digital services and government services • Trusted services • Digital ecosystems
Systems	• Data centers • Telecommunications networks • AI systems
Infrastructure	• Lands, buildings, structures, facilities • Access to infrastructure

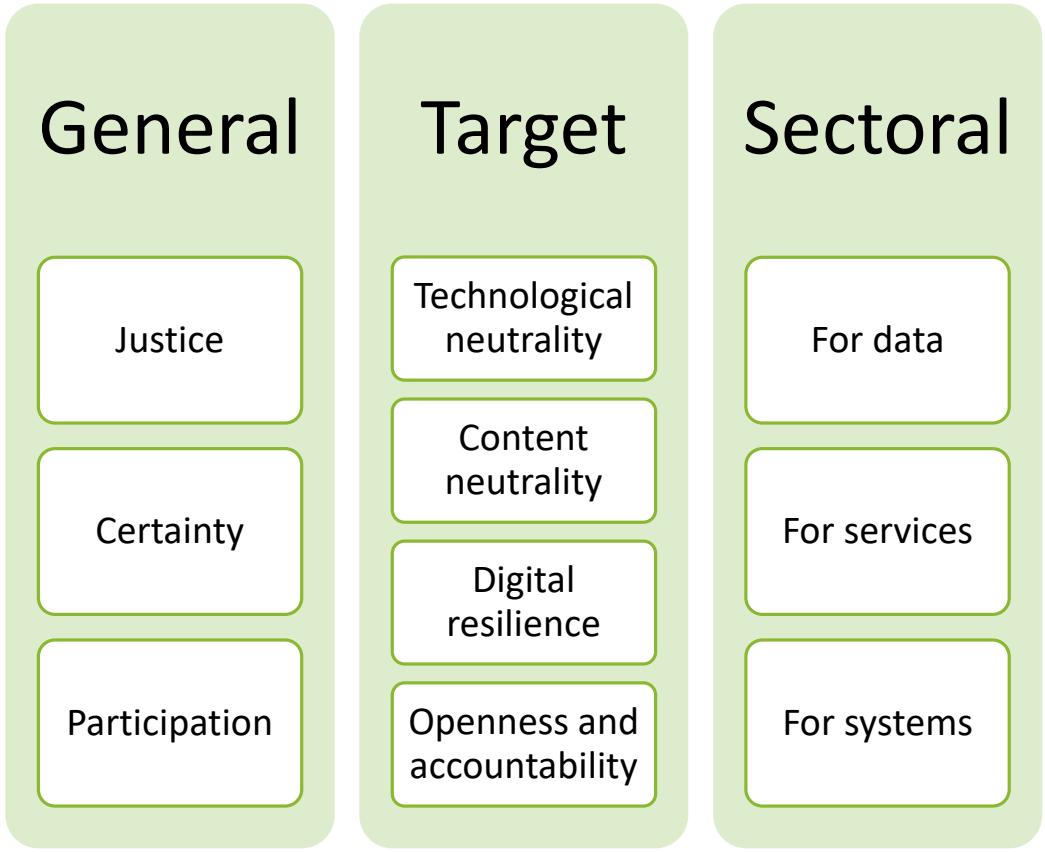
The main task of codification is to streamline social relations in the digital environment in such a way that the same rules apply to homogeneous relations, and different ones to heterogeneous ones. This required, first of all, the identification of four levels of regulation, each characterized by its own set of objects and relationships for their creation and use.

The multi-level nature of regulation responds to a multi-level model of digital relationships, where each next level appears as a result of relationships at the previous level. The rules for relations at each level are defined in the Special part

Levels of regulation



Principles of regulation



Social relations in the digital environment are developing rapidly, so legal regulation cannot cover all possible situations. As a basic framework for the subjects of relations in the digital environment and for regulators, the Code establishes principles, some of which define the foundations of legal regulation, the other part acts as a description of the target state that public relations in the digital environment should reach. Those principles that apply to specific areas of relations in the digital environment (for example, telecommunications or public services) will be disclosed in the Special Part of the Code

Method of regulaiton

Ownership

- The right to restrict access to their facilities
- The right to manage access to its facilities

Access

- Right of access to other facilities for the benefit of the community
- Non-discriminatory, fair and equal terms of access

The Code resolved the issue of its own method of regulation for the branch of digital law it created. The method of regulating relations in the digital environment is the establishment of:

1) the absolute right to the object (data right, which is analogous to the right of ownership), which implies that the owner of the object can manage access to the object, which creates conditions for investment in the digital environment;

2) limitations of absolute rights (access rights) established, as in the case of property rights, in the interests of the community and the development of the digital environment as a whole

Sources of norms

Code

- Has priority when regulating the digital environment
- Sub-law regulations are adopted only if provided for by the Code

Community rules

- Digital services rules
- Ecosystem rules

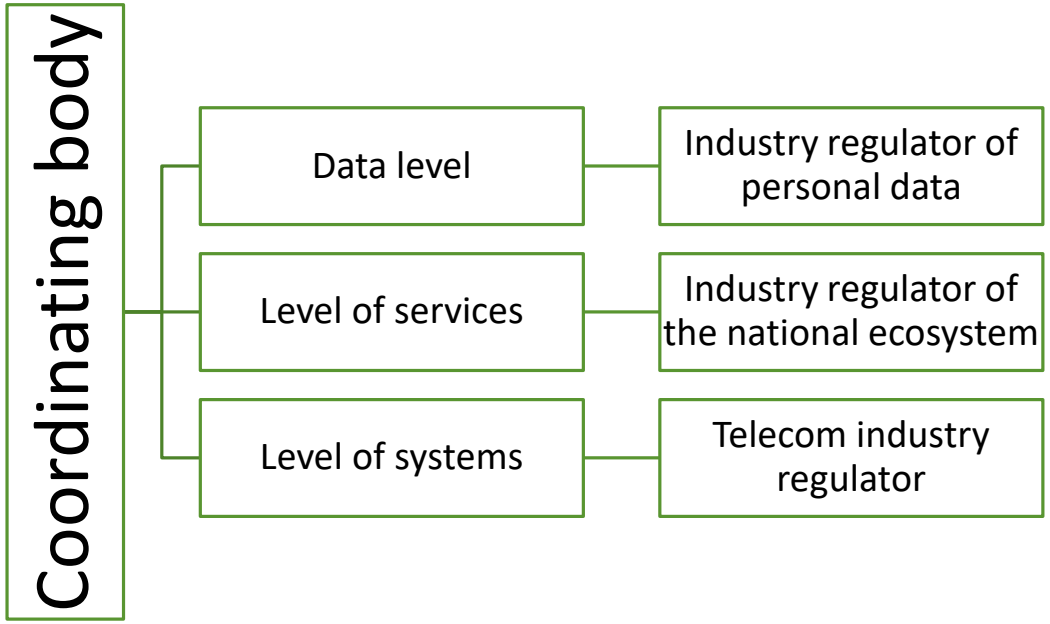
Internationally recognized practice

- International standards
- Recommendations of international organizations

The Code takes into account the structure of the sources of legal norms that has actually developed in the digital environment. In each state, its legislation has priority, both citizens and foreign investors are guided by it, therefore it is important to establish clear and accessible rules and limit departmental rule-making.

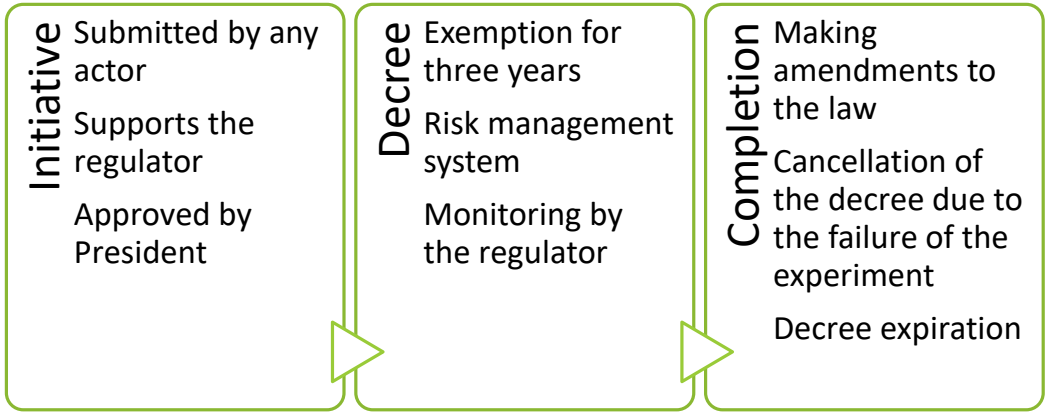
However, national legislation cannot ignore the rules by which the digital environment lives: they are formed by the rules of various digital communities, as well as various standards and recommendations by which technologies are built and interact.

Regulator system



To ensure long-term stability of regulation, the Code does not empower a specific state body. Instead, the Code defines the content of digital governance powers and the requirements for the authorized state body to exercise these powers. The specific body or bodies shall be determined by the Cabinet of Ministers in accordance with the actual needs of digital development

Special regulation



The President may temporarily release subjects of legal relations in the digital environment from certain obligations established by law in the manner prescribed by the Code.

The purposes of special regulation include:

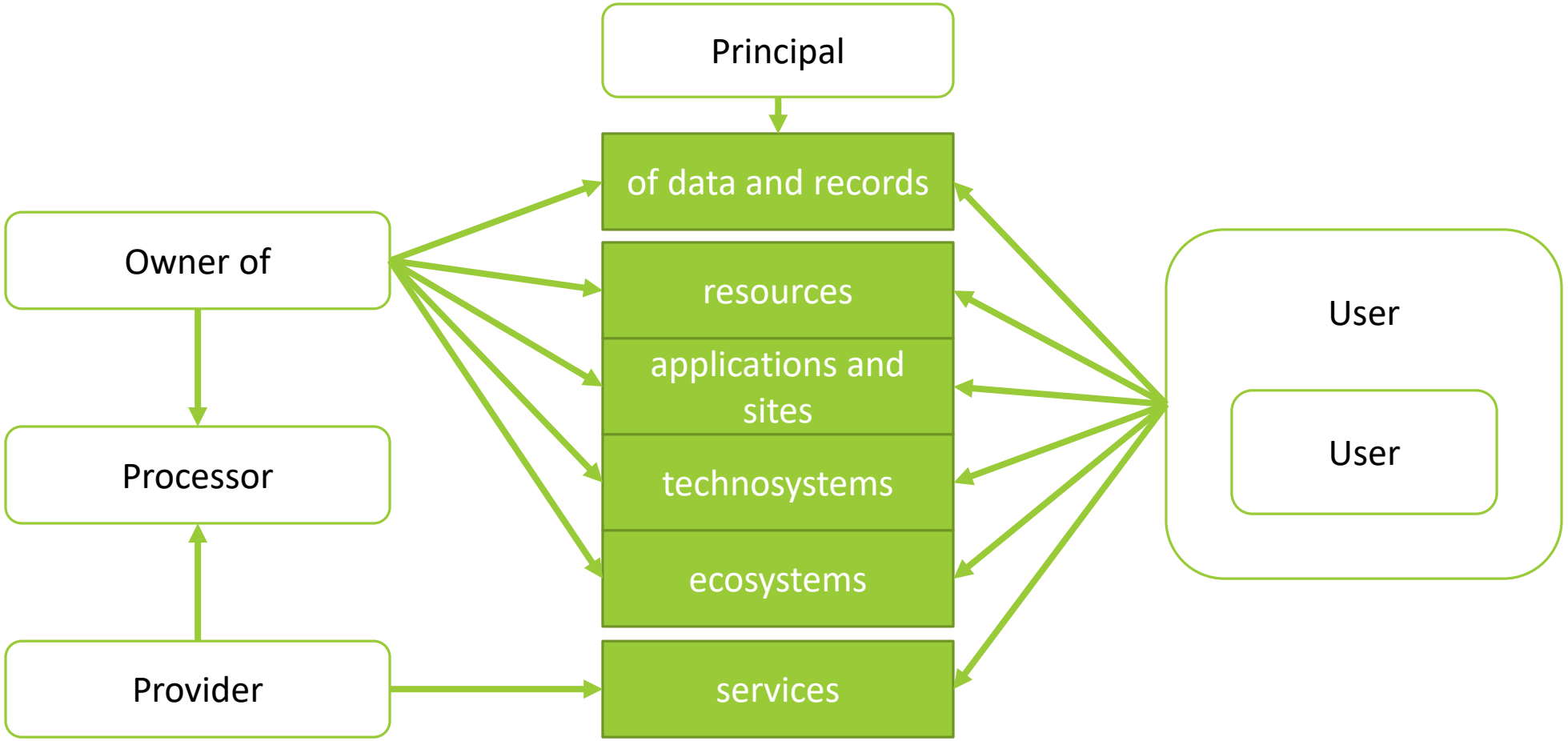
experiments and testing of digital innovations in a real-world environment;

Improving the quality and availability of digital resources and services;

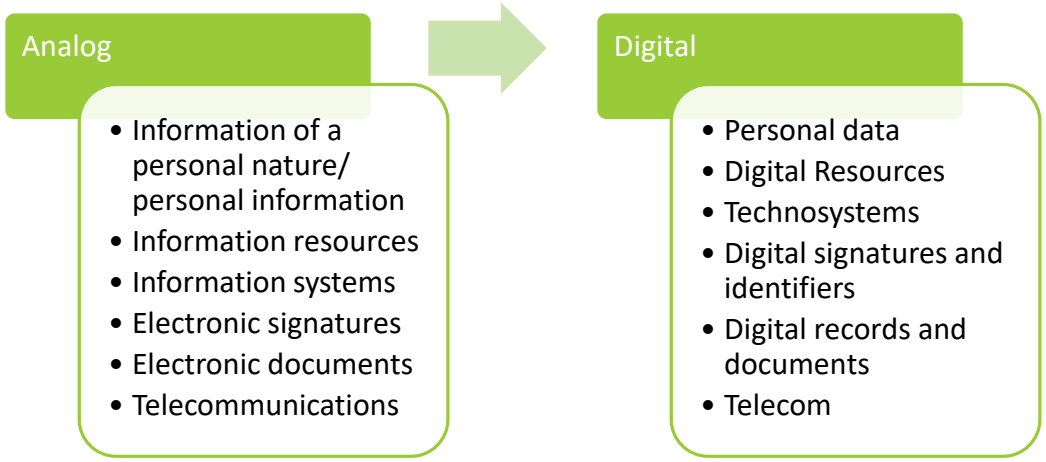
Promoting fair competition and better governance;

Attracting investment in the digital economy

Objects and subjects

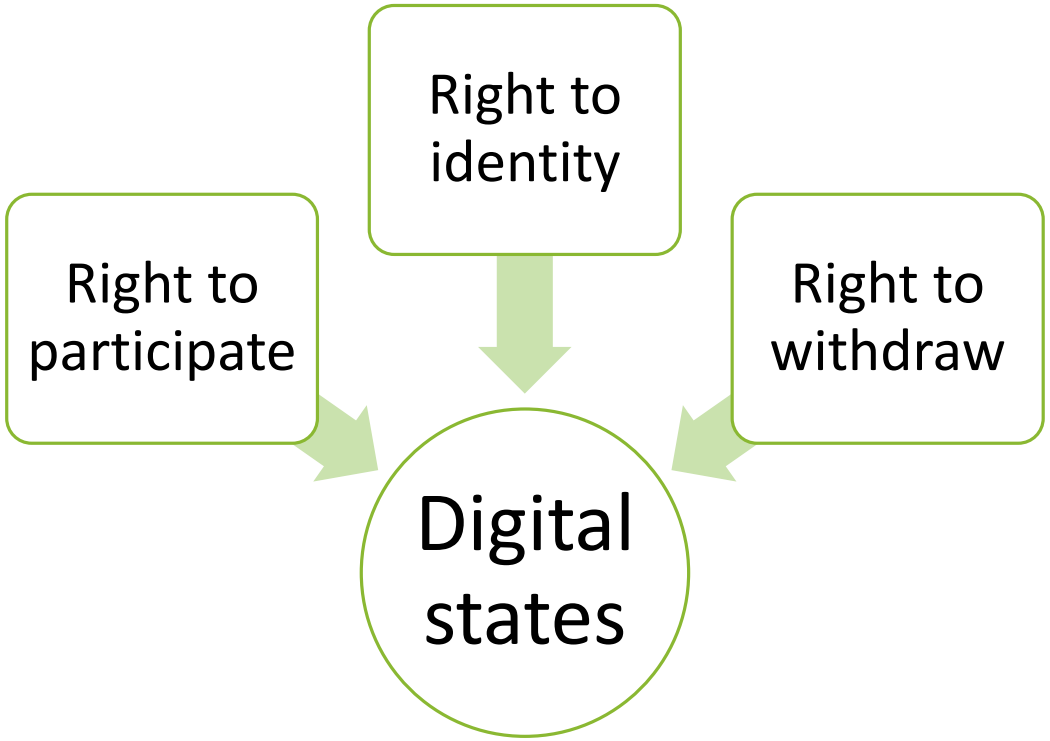


“Old” and “New” objects: ensuring backward compatibility



The Code’s objectives are, on the one hand, to ensure the speedy transition to digital governance as the most effective phase of public administration, and on the other hand, to ensure the sustainability of the existing regulatory system. Therefore, rules relating to aging objects such as information resources on non-digital media, electronic documents outside the digital resources, analogue telecommunication networks and services, while creating certainty regarding their use, are aimed at stimulating their modernization or abandonment. Information systems are no longer regulated by the Code (due to the regulation of digital technology systems)

Digital citizenship



Participation in the digital environment, in the creation and development of digital communities, on the one hand, is an inalienable right of everyone, on the other hand, is a necessary condition for development of the digital environment. Therefore, the Code not only endows the subjects of relations in the digital environment with the necessary rights (and imposes appropriate duties on them), but forms a stable legal relationship between the subjects and the digital environment generated in relations between them - digital citizenship.

The Code also describes the main legal statuses (roles), in which the subjects of relations in the digital environment may be found

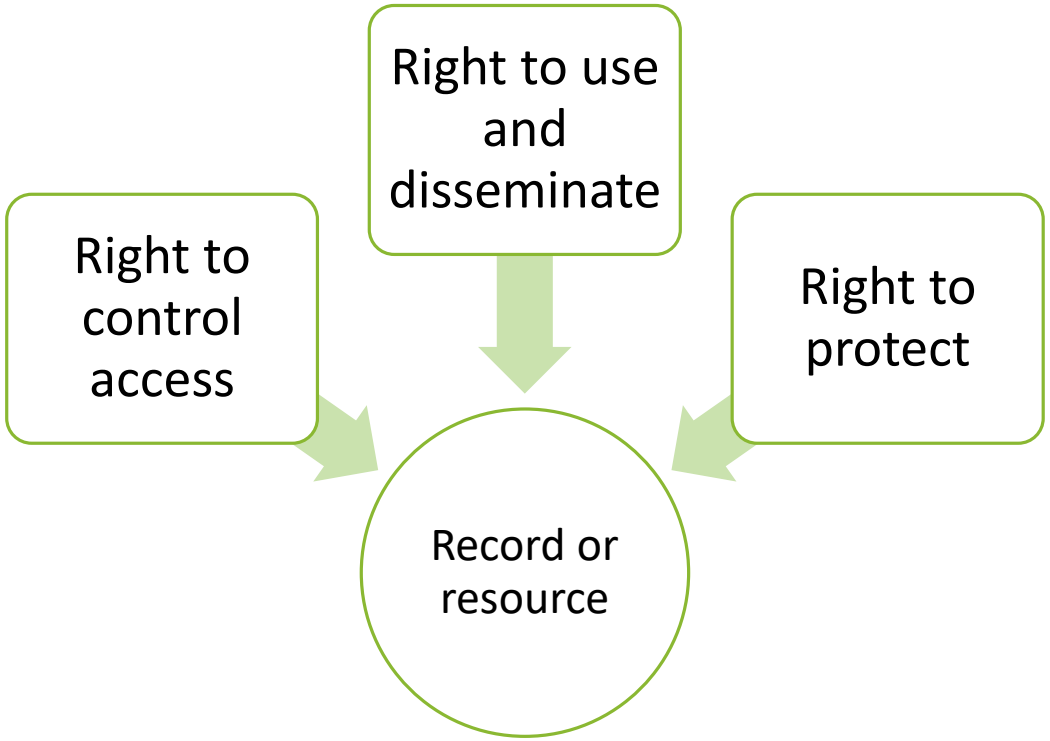
The right to identity and depersonalization

Participation in digital communities, use of digital services, etc. only possible if data about the subject is processed

If the data are not processed in the interests of the subject, identifiers should be removed from them, which allow combining data from different sources, for example, e-mail

The data remain personal, but:
1) they can be processed without consent;
2) in order to claim rights to them, the subject should prove that these are his data

Digital rights



Digital rights are established as an implementation of a digital law method and provide protection for investments in digital rights objects and the possibility of circulation of such objects. Digital rights are established independently of property rights and exclusive rights, although their exercise should comply with the restrictions established by law. Digital rights may be held jointly by more than one person.

The Code provisions are aimed at maintaining a balance of interests between digital rights holders and data principals, that is, those to whom the records relate.

Digital recording on legal facts

Digital records as grounds for the emergence, change, and termination of legal relations in the digital environment

Grounds for the emergence, change, termination of legal relations in the digital environment shall be legal facts expressed in digital records, including those presented in the form of digital documents or as part of digital resources

The Code establishes rules to balance the interests of the parties to the relationship when using modern digital tools such as smart contracts, digital signatures, stamps and other trusted services, as well as when making decisions automatically.

The Code offers a mechanism similar to the eIDAS Regulation in the European Union or the UNCITRAL IdM Model Law, which allows using the results of using foreign services as grounds for the emergence, change, and termination of legal relations in the digital environment

Excercision of digital legal relations

Restriction of Distribution of Digital Records and Access to Digital Records

1. Access to or distribution of digital records may be restricted in accordance with the metadata of such records only on the basis of the law only in the following cases:

1) if the restriction of access is the exercise of digital rights;

2) if the metadata of digital records indicate that they are classified as a legally protected secret;

3) if the distribution of digital records or access to them is prohibited by a court decision in accordance with the law.

2. The restrictions introduced should comply with the principles of regulation of relations in the digital environment. Arbitrary restriction of access to digital records and their distribution is not allowed.

As part of the implementation of the principle of content neutrality, the Code establishes a presumption of public availability of digital data. Restrictions on their distribution and access to them can be established in a closed list of cases and must be reflected in the metadata of the corresponding digital records.

Codification preserves and expands the provisions of the current legislation on open data and on access to information held by public authorities

Digital resilience

Digital resilience

The exercise of rights and fulfillment of obligations in the digital environment depends on trust in the objects of relations in the digital environment, that is, on the completeness, reliability and relevance of the digital records used, the availability and reliability of digital services and digital technological systems. In order to ensure trust in the objects of legal relations in the digital environment and minimize the negative consequences of incidents in the digital environment that lead to incompleteness, inaccuracy, irrelevance of digital records, unavailability or disruption of the functioning of digital services or digital technological systems, the subjects of relations in the digital environment ensure the long-term stability of relations in the digital environment (digital resilience).

The Code establishes digital resilience as a priority for digital management. This reflects the emerging understanding in modern science of the impossibility of 100% protection from incidents in the digital environment and the need to spend the resources of society to minimize the number of incidents and to quickly overcome their negative consequences. The Code is based on a risk-based approach, as well as by design approaches that provide for the design and control of measures to ensure digital resilience at all stages of the life cycle of a particular technology

Sections of the Code

General part	Digital data and resources	Digital Services	Technosystems
▪ Scope, method, principles and sources ▪ Regulators ▪ Special regimes ▪ Digital interaction ▪ Digital identity ▪ Relationships in digital environment: actors, objects, legal grounds ▪ Digital resilience	▪ General provisions on the regulation of BigData and the Internet of things ▪ Personal data ▪ Spatial data ▪ Digital technological resources, including telecommunication resources	▪ General provisions on digital services ▪ State services and the national digital ecosystem ▪ Digital Wellness Services ▪ Trusted services ▪ Telecommunication services	▪ General provisions on digital technological systems ▪ Telecommunications networks ▪ Artificial Intelligence Systems

Digital data

DIGITAL RECORDS, DIGITAL RESOURCES

Data processing and digital resources

General Provisions

- Big data technology
- Internet of things
- Prohibition of Unfair Processing
- Access to own data
- Correction and addition

Personal data

- Principles and bases of processing
- Special data categories
- Deletion, objection to processing, restriction of processing
- Processor involvement, joint processing
- Cross-border transfer
- Powers of the body
- Features of non-automatic processing

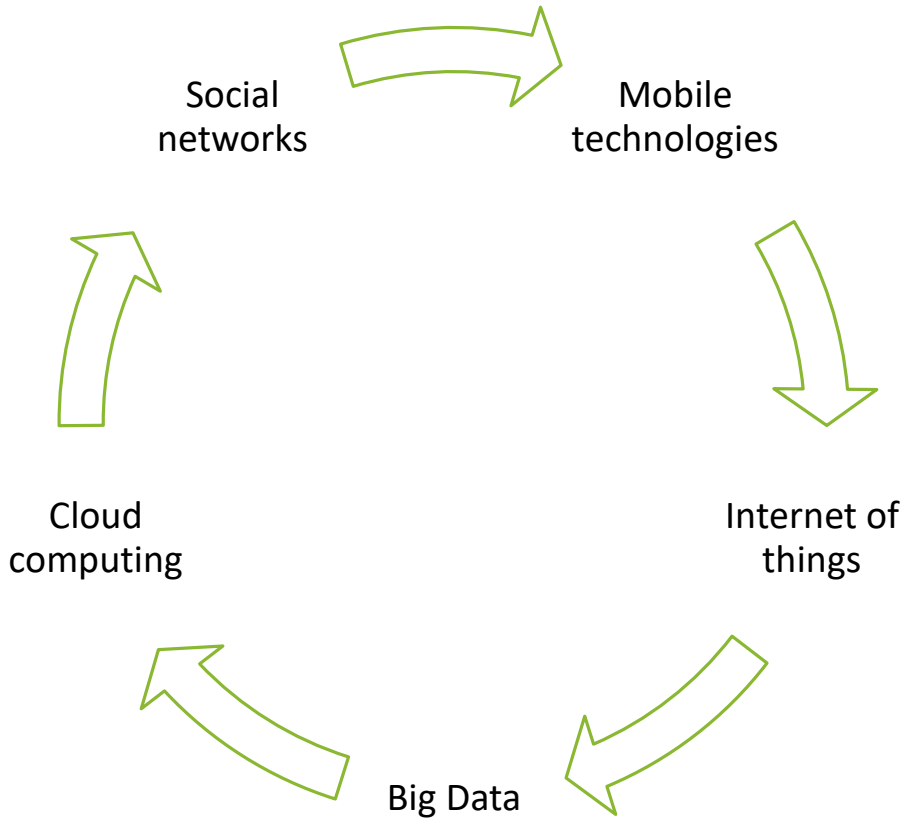
Spatial data

- Types of spatial data
- Spatial metadata
- Geo-resource and funding mechanism for spatial data digitization
- Geosite and digital cartographic basis
- Compatibility and portability

Digital technical resources

- Radio frequency resource
- Numbering resource
- Internet addressing resource
- National ecosystem element resource

Data processing technologies



Mobile devices predetermine the importance of information about the location of objects: from roads to cars;

IoT devices generate data about the world all the time;

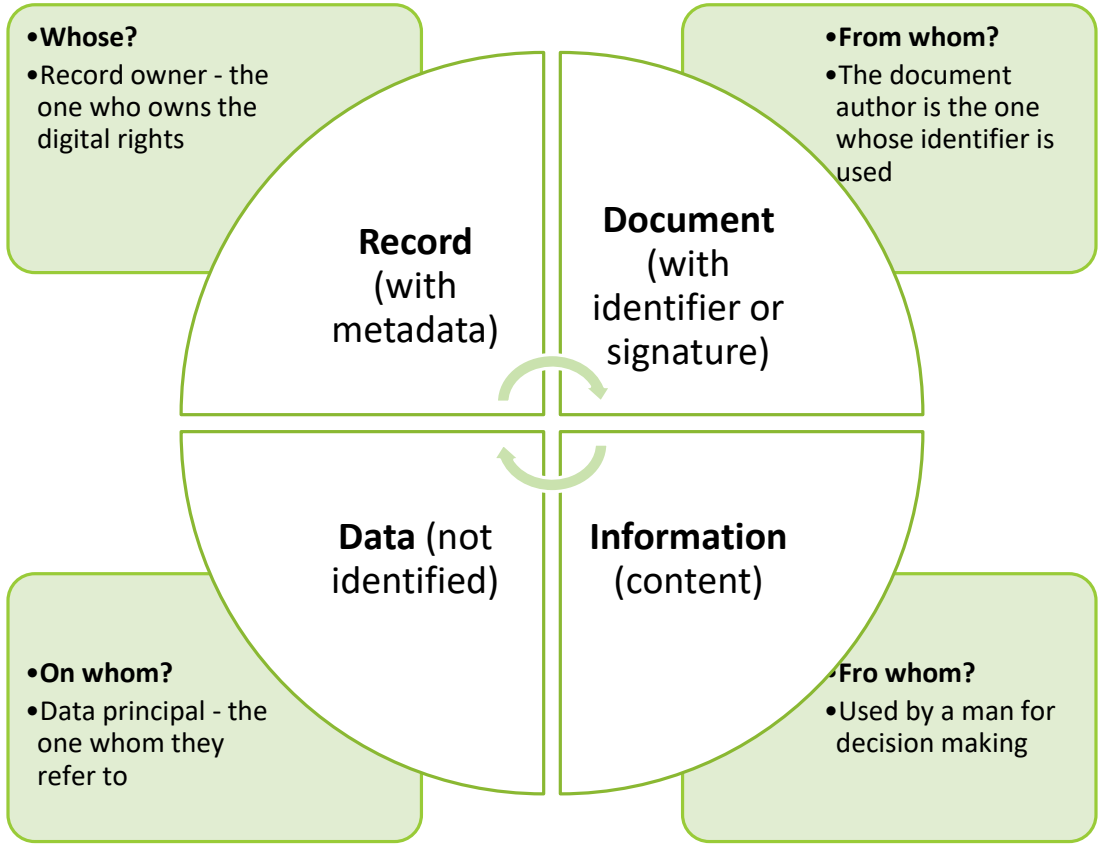
The data arrays are analyzed using the Big Data technology;

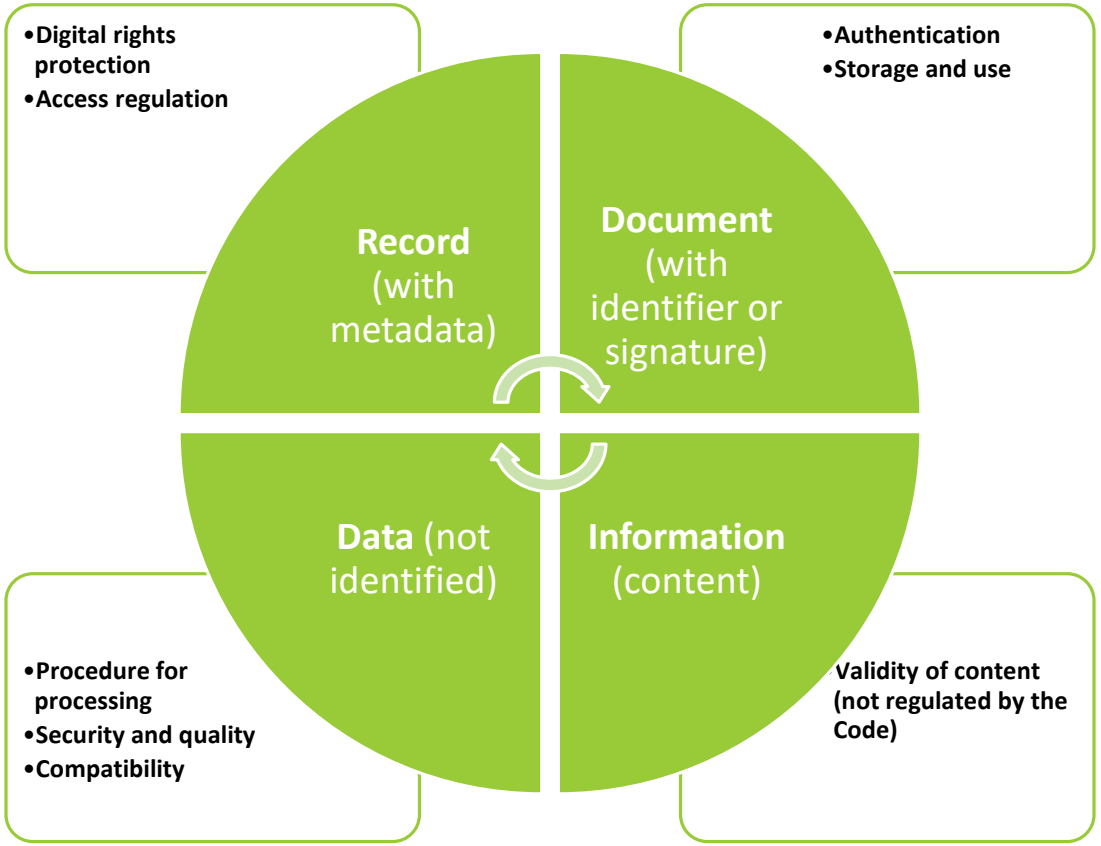
Storage and access to knowledge from any location is possible using the cloud solutions;

Sharing this knowledge and working together on them is convenient in messengers and social networks;

Which are analyzed using Big Data technology, which leads to the emergence of more and more convenient and effective mobile devices and cloud solutions

Regulation and lifecycle of digital data





Personal and non-personal data

DATA PRINCIPAL

Any person to whom the data relates (individual, organization, government agency)

The right to receive information about the processing of data about oneself (who processes and how)

The right to receive a copy of his/her personal data

The right to clarify and supplement data about oneself

Protecting interests in relation to the “digital twin” of oneself or one's digital devices

SUBJECT OF PERSONAL DATA

Individual to whom the data relate

Closed list of reasons for processing

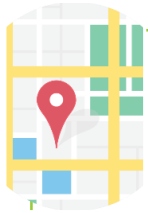
Right to object

Right to delete

Protection against personal harm in data processing

Spatial data in the digital economy

DATA TYPES



About the location (about coordinates) - clinics and cafes, buses and utility vehicles, that is, everything that we use in everyday life

Cartographic (on the relative position of objects on the ground and their sizes) - data necessary for orientation in space and measurement of dimensions

Geodetic (building of the Earth) - basic scientific data necessary for environmental protection and research

ACCESS TO DATA

Cartographic Fund managed in accordance with geodesy and cartography legislation

Digitization of paper maps and creation of digital cartographic products

Search for existing and adding new digital spatial data within a **georesource**

Presentation of data on a digital map and interaction through API using a geosite

Digital Technological Resources

Right to use radio frequencies	Digital radio frequency resource
Right to use numbering	Digital numbering resource
Right to address Internet	Internet addressing digital resource
The possibility of using digital resources, services and systems of the national digital ecosystem	National ecosystem element resource

The Code contains a mechanism for securing rights to objects of legal relations in the digital environment, similar to the Real Estate Register. The radio frequency resource and numbering resource belong to the Kyrgyz Republic, but the right to use frequencies or numbering belongs to the principal of the corresponding entry in this resource (that is, to the person whose right is recorded). The Internet addressing resource is maintained in accordance with generally accepted international practice

The resource of elements of the national ecosystem secures the right to interact within the framework of the national ecosystem with the object of legal relations in the digital environment, which is recorded in the resource

Digital Services

TRUSTED SERVICES, STATE SERVICES, NATIONAL ECOSYSTEM

DIGITAL WELLBEING SERVICES, TELECOM SERVICES

Digital service regulation

General Provisions

- Principles
- User Agreement
- User protection
- Protection of competition

Trusted services

- Digital authentication services
- Digital signature
- Digital archives
- Foreign trusted services

Digital Wellness Services

- Digital services in medical care
- Digital Wellness Devices
- Features of data processing and use of AI

State services and the national ecosystem

- Rules of creation and use of state services
- Factory of Public Services
- Tunduk and interaction rules
- National ecosystem rules

Telecom services

- Supplier responsibilities
- Rights and obligations of users
- Secrecy of telecommunications
- Special services

Trusted services

Providing identity of the subject

- Digital identification systems: define the rules for obtaining and using digital identifiers, including when creating digital records
- Digital authentication services: allow to verify the identity of the actor in the digital environment

Ensuring the immutability of documents

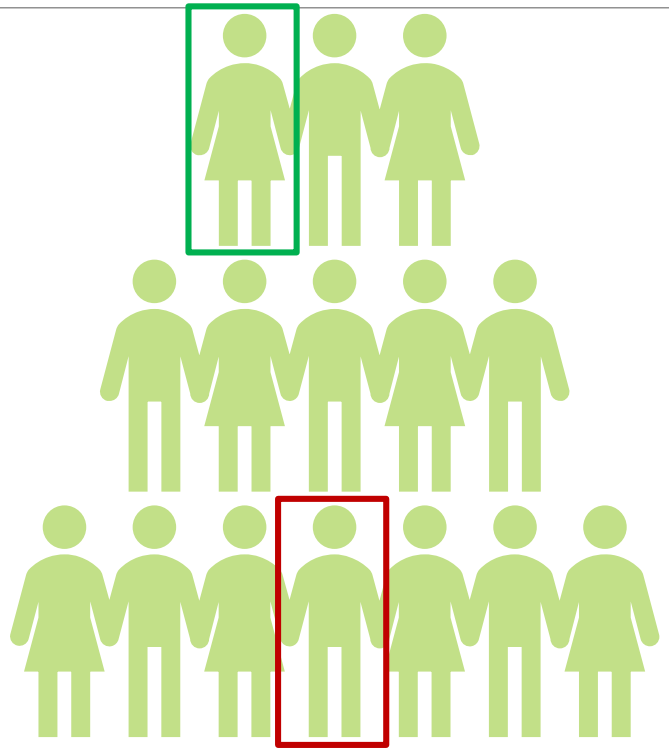
- Digital signatures of individuals
- Digital seals of organizations
- Digital archives
- Guaranteed message delivery services (within government digital services)

Providing confidence in infrastructure elements

- Web Authentication Services (HTTPS) - provided by foreign suppliers

difference?

Identification



Definition

"Who is this from among unknown person?"

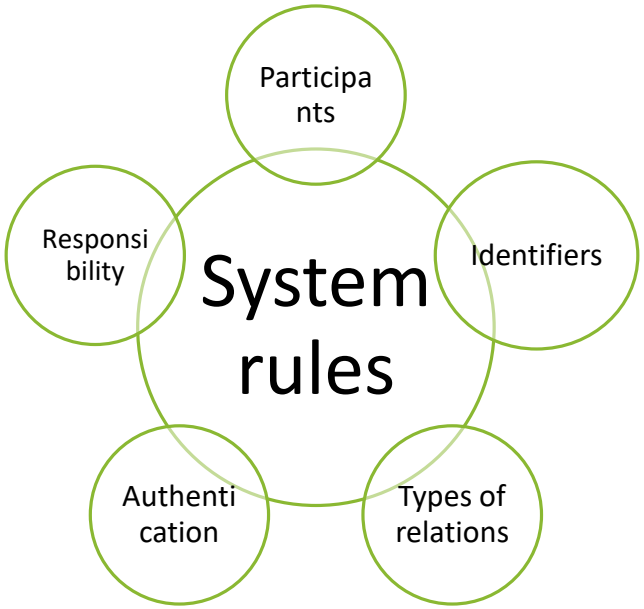
Authentification

Confirmation

"Let's make sure it's you"

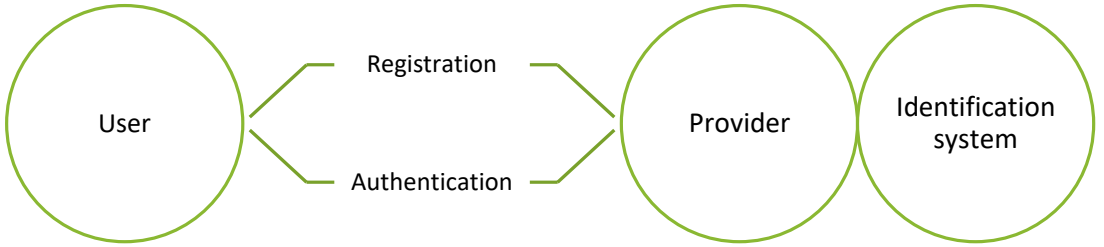
Identification systems and authentication services

IDENTIFICATION SYSTEM



Examples: Unified identification system, biometric recording system

AUTHENTICATION SERVICE (BASED ON IDENTIFICATION SYSTEM)



Examples: SMS authentication

Identifiers

Individual

- last name, first name, patronymic, date of birth
- personal identification number
- qualified electronic signature
- contact information (subscriber number)

Identifier – *information that allows connecting people and organizations to digital records*

Digital recording

Legal entity

- taxpayer identification number
- main state registration number/ code of a foreign organization
- qualified electronic signature
- Electronic seal

Digital documents

With the identifier	With unqualified signature (stamp)	With the qualified signature (stamp)	With guaranteed delivery	In the digital archive
Digital record where the identifier is used according to the rules of the identification system - a digital document (for example, a record in a registry with a unique number)	A digital record corresponds to a signature whose certificate is issued by a non-accredited CA. Such record shall be considered a digital record if so provided by the NLA or contract	The digital record corresponds to the signature issued by the accredited CA. Such a record is considered a digital document, unless expressly excluded by law (for example, a will)	Information about receiving notifications to the personal account on the public services portal will be recorded and can be used as evidence	The legal force of the document (digital initially or scanned duplicate) is ensured by guarantees of immutability and verifiability within the technological system of the archive

Legal force of digital documents

Making digital documents legal

With cryptography (EDS)

Unqualified signature or seal	Qualified signature or seal
Legal significance is recognized where there is an NLA or agreement of the parties providing for verification of the digital signature	Legal value recognized in all cases (except for legislative prohibition of digitization of the document)

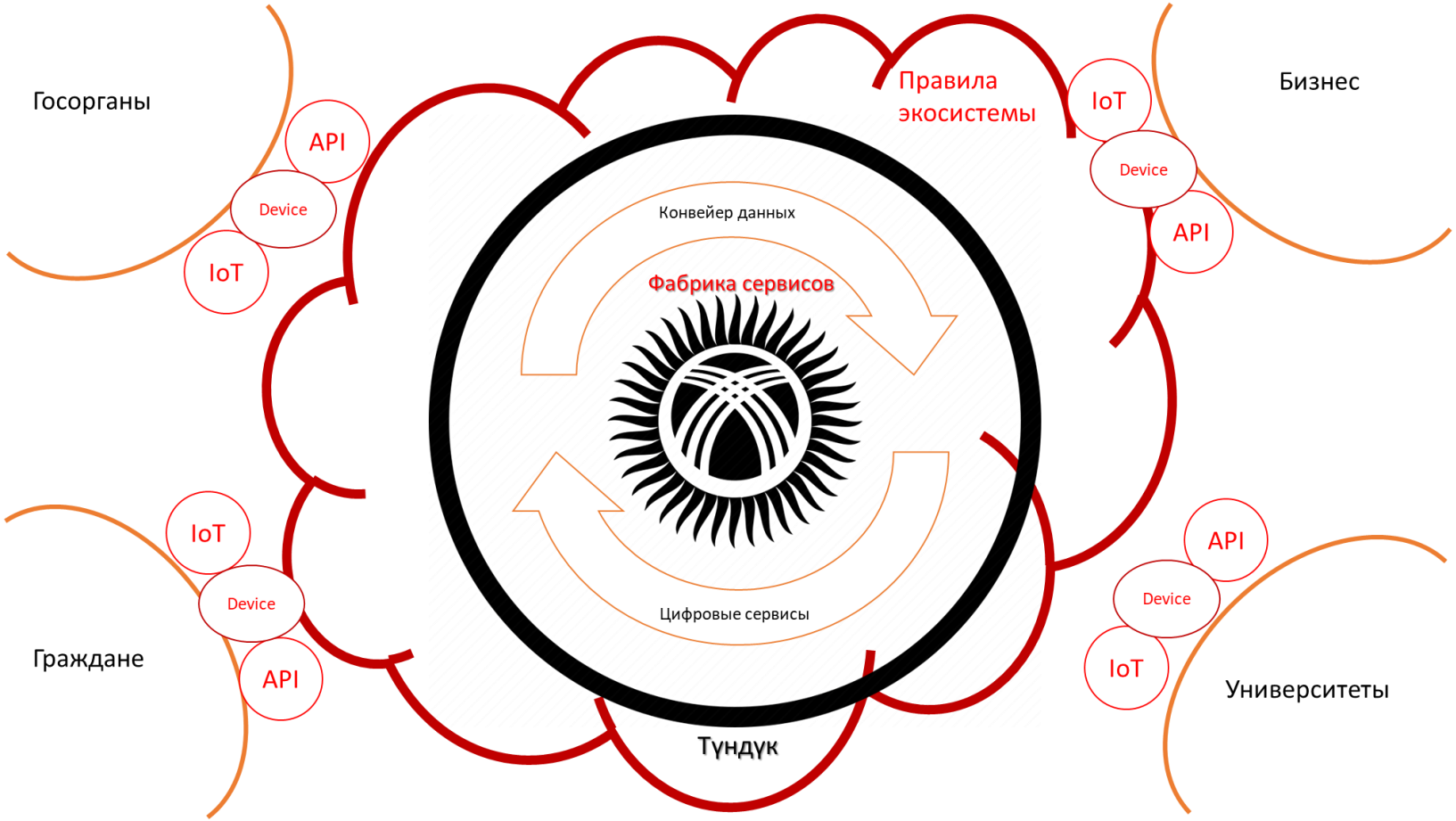
Without cryptography

Use of identifier in digital record according to identification system rules
Legal significance is recognized if the identifier is indicated in the digital record itself or used in its creation, as indicated in the metadata

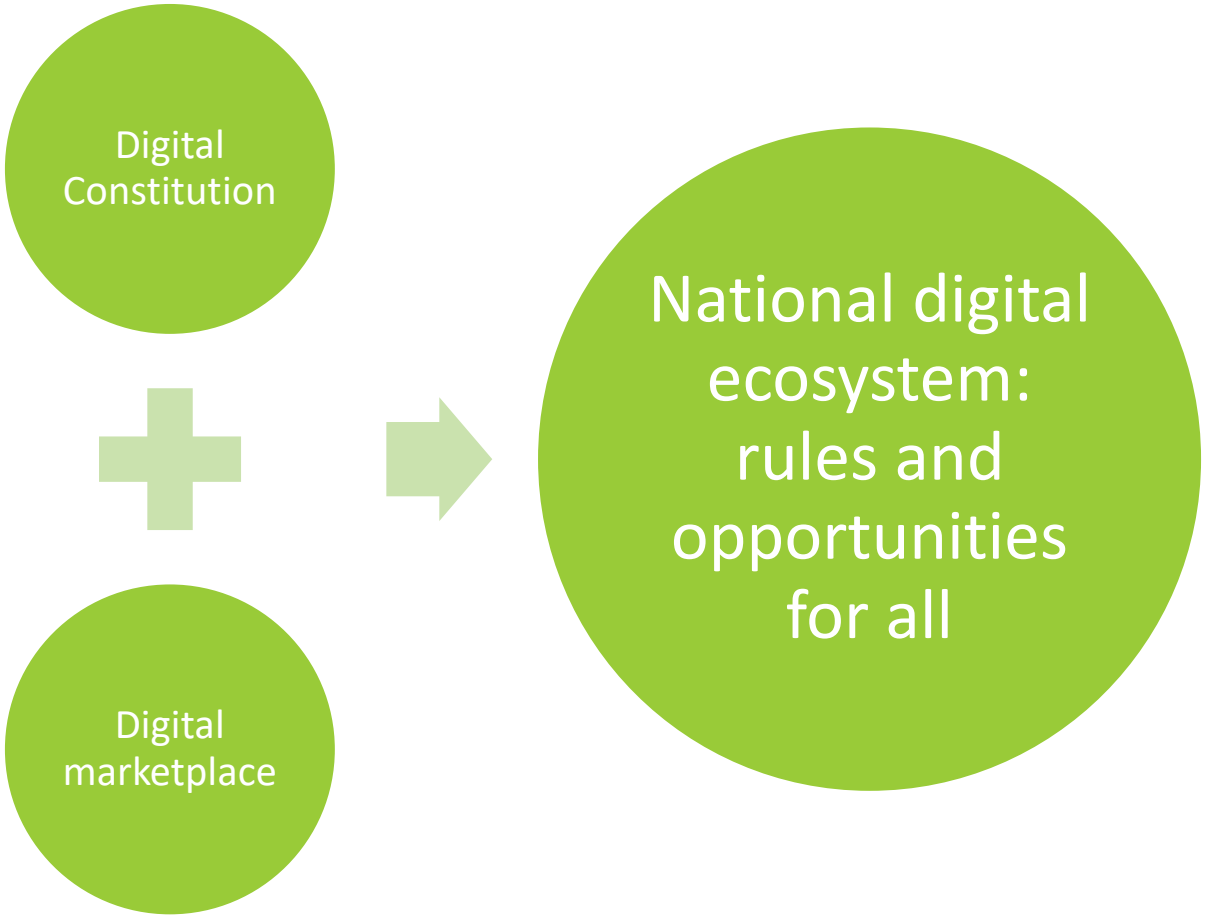
Marketplace of public services

Store	Supermarket	Marketplace
		
Each supplier is his own boss, he produces or buys everything himself, he determines the terms of sale. To collect a basket, you need to go between different stores Advantage: Supplier understands his products Disadvantage: It takes a lot of time to stand in lines	Suppliers agree with the owner of the supermarket to place on shelves. Supermarket owner determines product requirements Advantage: Buyer can get everything he wants quickly and in one place Disadvantage: everything is decided by the supermarket owner, who does not need competition between suppliers	The owner of the marketplace determines the trading rules. Any supplier can offer their goods even if others are already selling them. Buyer can find and quickly compare goods Advantages: suppliers compete directly for the buyer and compete for the quality of their products

National digital ecosystem



Code as an ecosystem



Digital Technological Systems

TELECOMMUNICATIONS NETWORKS. ARTIFICIAL INTELLIGENCE

Digital Technosystems and Networks

General provisions

- Status of system owner and network operator
- Systems interaction
- System placement
- Systems security

State policy

- Principles of development of technosystems
- Industry regulator
- Commission on Radio Frequencies
- International cooperation

Interaction with state bodies

- Licensing
- Interaction with law enforcement agencies
- Antimonopoly and tariff regulation
- Broadcasting

Artificial intelligence

- Principles, requirements and limitations
- Hazard assessment of AI systems
- Risk management
- Provision of specified characteristics and documentation of AI systems
- Data quality management for AI
- Responsibilities of owners and users

Digital service

- Opportunities available to users to use digital technological systems in order to: 1) create, process, store the digital data or access to them; 2) exchange digital data with other users, including by accessing digital data uploaded or created by other users

Digital technosystem

- System of digital devices, computer programs and databases for digital data processing

Digital resource

- An streamlined set of digital records, including a database designed for the storage and use of digital records and (or) digital data and access to them

Telecommunication service

- Opportunities available to users to use digital technological systems to exchange digital data with other users, including by accessing digital data uploaded or created by other users + voice connection (backwards compatible)

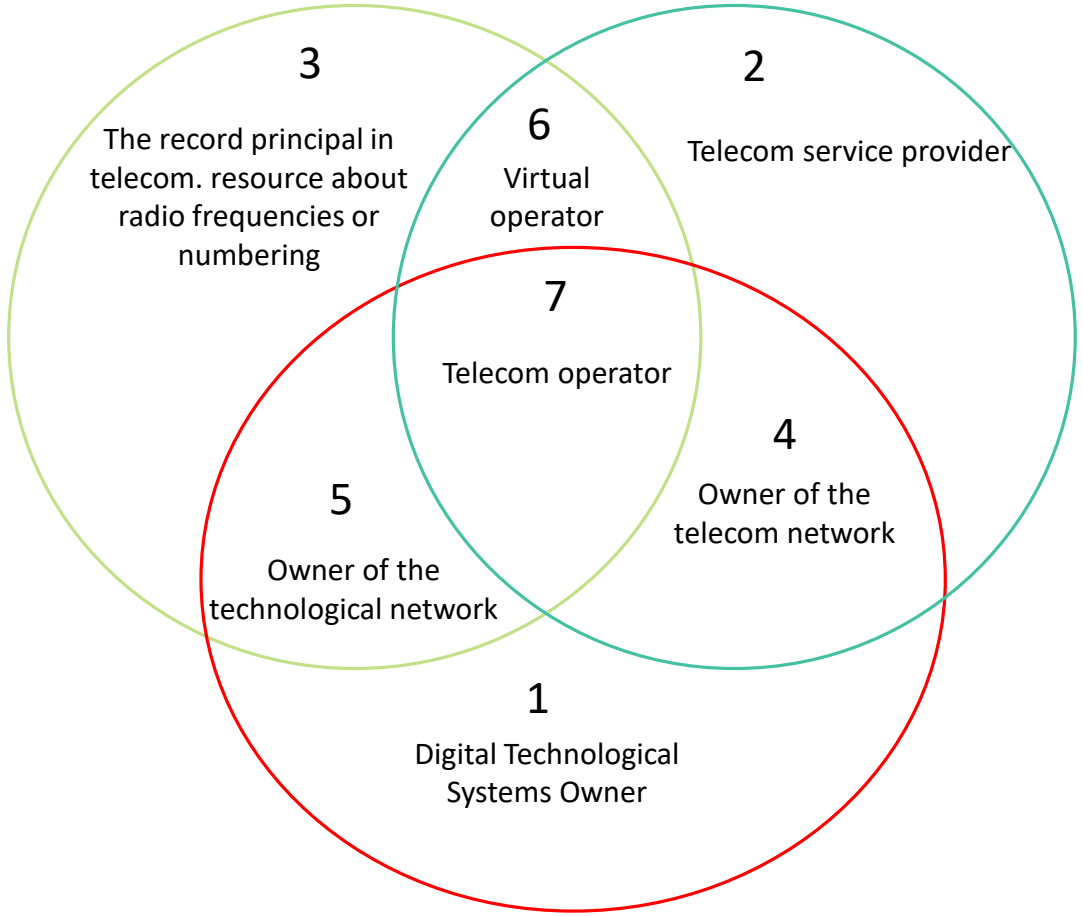
Telecommunications network

- Digital technology system designed to provide telecommunication service

Telecommunications resource

- A digital resource designed to store and use digital records of the rights to use radio frequencies, numbering and addressing, and access to them

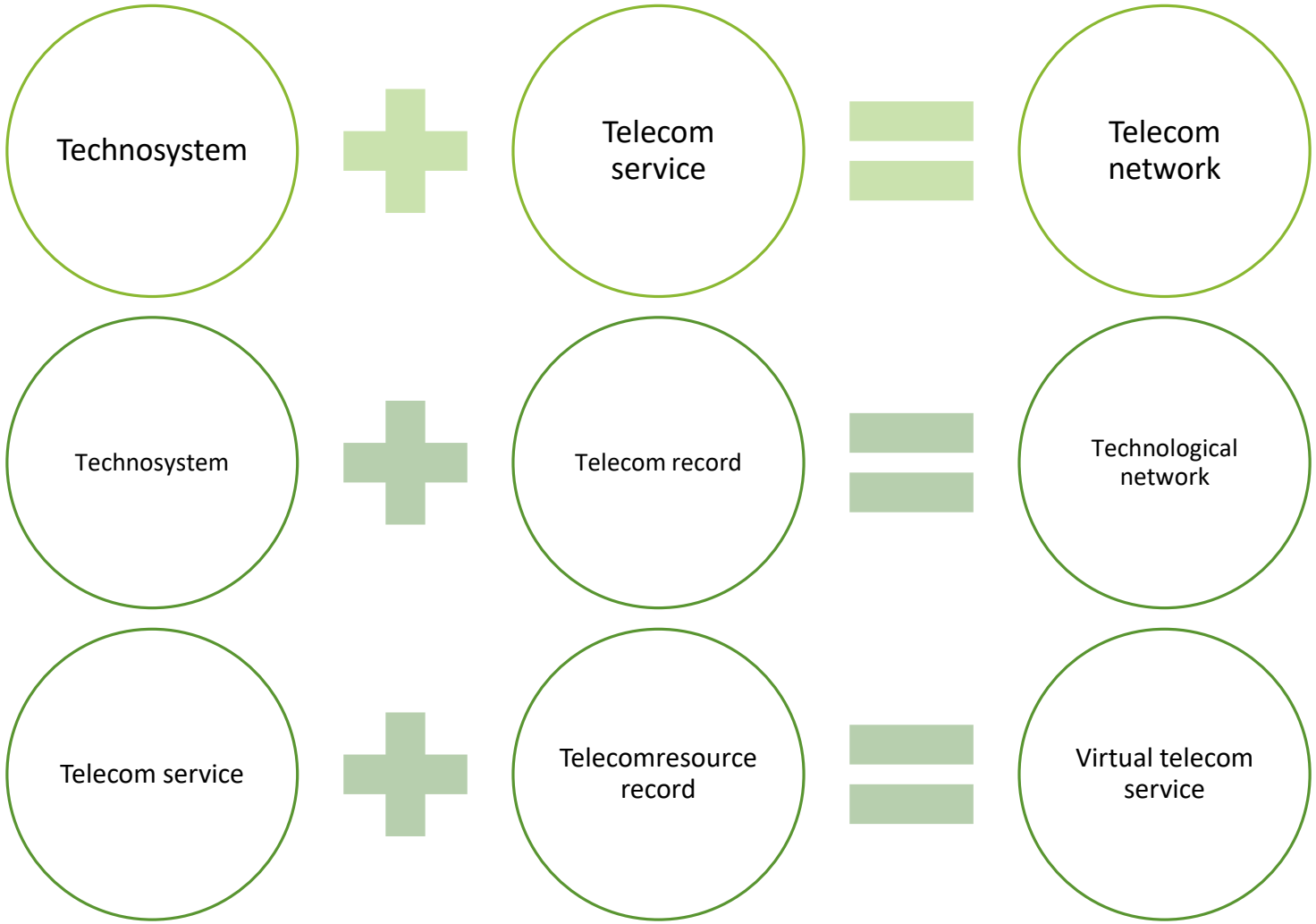
Concept system

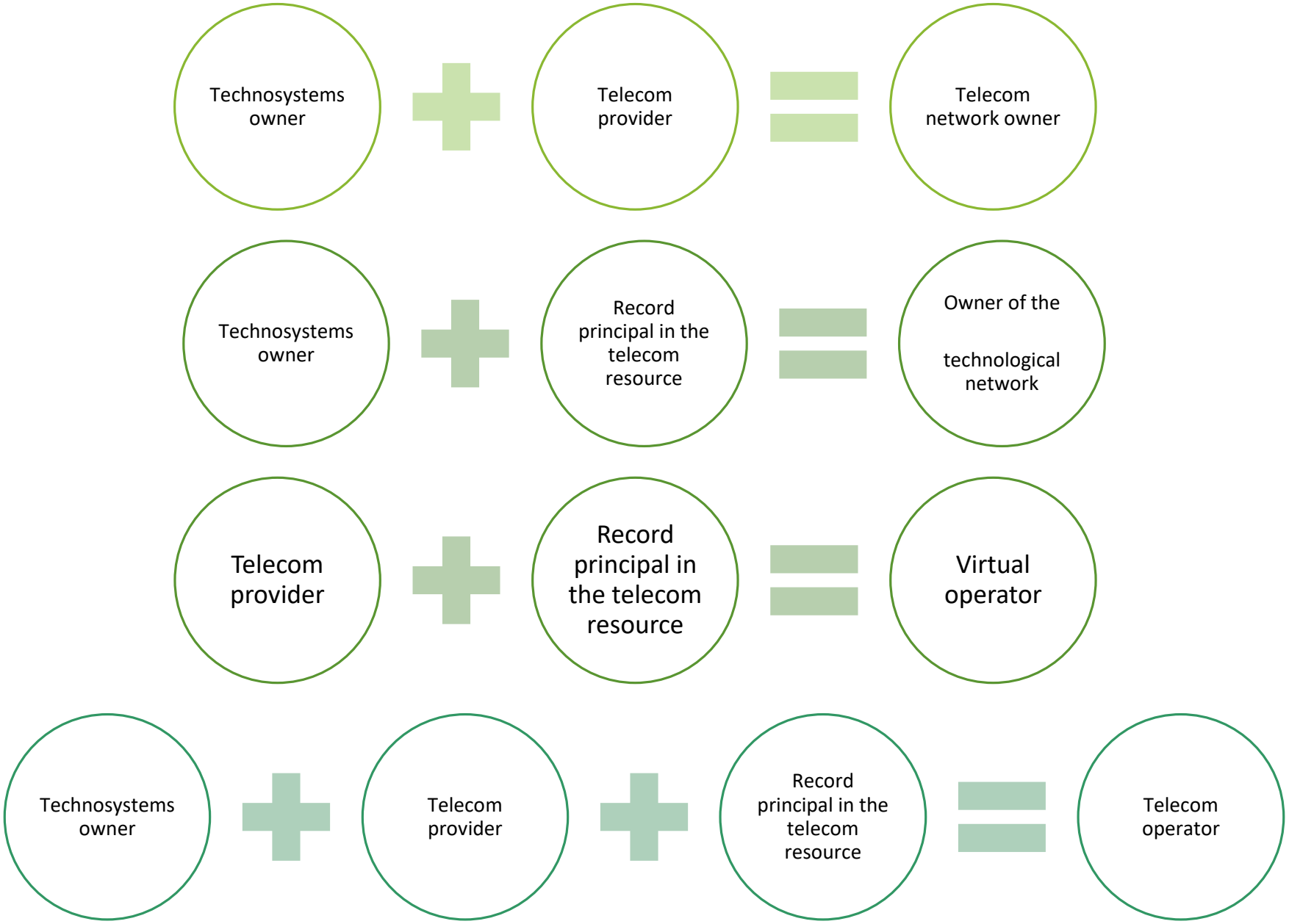


resource

service

system


Technosystem
Telecom service
Telecom network
Technosystem
Telecom record
Technological network
Telecom service
Telecomresource record
Virtual telecom service


Technosystems owner
Telecom provider
Telecom network owner
Technosystems owner
Record principal in the telecom resource
Owner of the technological network
Telecom provider
Record principal in the telecom resource
Virtual operator
Technosystems owner
Telecom provider
Record principal in the telecom resource
Telecom operator

Artificial Intelligence technosystems

RESTRICTIONS ONLY FOR AI SYSTEMS:

- Knowingly violating the law (prohibited)
- Of high risk
- interacting with a person
- Implementing deepfakes
- Used in public administration

DISCLOSURE OF INFORMATION ON AI:

- Publication of the declaration of conformity
- Explicit reporting of AI use
- Duty of effective human control
- Technical documentation
- Selfregulation

High risk AI systems

THE OWNER ASSESSES WHETHER THE USE OF AI INCREASES THE RISK FOR:

- Human life and health;
- Human and civil rights and freedoms
- Environment
- Defense capability of the state
- National security
- Public order and morality

FOR HIGH-RISK AI SYSTEMS - ADDITIONAL. REQUIREMENTS:

- To risk management
- To the required characteristics of AI systems
- To digital data quality for AI systems
- To the technical documentation on the AI system

Requirements of openness, understandability, control, accuracy, reliability, digital resilience