Talking Interoperability

In Focus | Belgium

Digital Convergence
USP2030

Digital Convergence
USP2030

The Digital Convergence Initiative (DCI)

A joint effort by USP2030 members and non-members, governments, development partners and private sector towards creating a harmonized and interoperable digital ecosystem for social protection

Building consensus-based standards for interoperability to….

- …foster an ecosystem for innovation by ICT solution providers to build products that are interoperable, easy to use, integrate, maintain and scale based on globally agreed standards and guidelines
- …reduce time and costs of developing solutions at the country/program level
- …enable programs and countries to mix and match different components from various vendors or develop them in-house, as standards-based modules are inherently interoperable
- …ensure that systems are future-proof by design, regardless of current levels of policy and information systems maturity

Digital Convergence
USP2030

Talking interoperability

A monthly dialogue series by the DCI to facilitate in-depth technical conversations around integrated and interoperable SP information systems across countries

Deep dive into one country-level system per session to…

- … share nuts and bolts of how agencies have designed their social protection information systems for interoperability
- …understand how agencies have tackled the major challenges to interoperability.
- ….brainstorm potential solutions to remaining bottlenecks

Digital Convergence
USP2030

Presenter

Frank Robben

General Manager, CBBS & the eHealth-platform

Discussants

Ernesto Brodersohn

ISSA Senior Official in Charge of ICT Technical Commission

Anita Mittal

Senior Advisor, Digital Convergence Initiative, GIZ

Moderator

Valentina Barca

Independent Consultant, Social Protection

Digital Convergence
USP2030

Principles of good eletronic information management in the social sector

frank.robben@mail.fgov.be

@FrRobben

https://www.frankrobben.be
https://www.ksz.fgov.be
https://www.ehealth.fgov.be

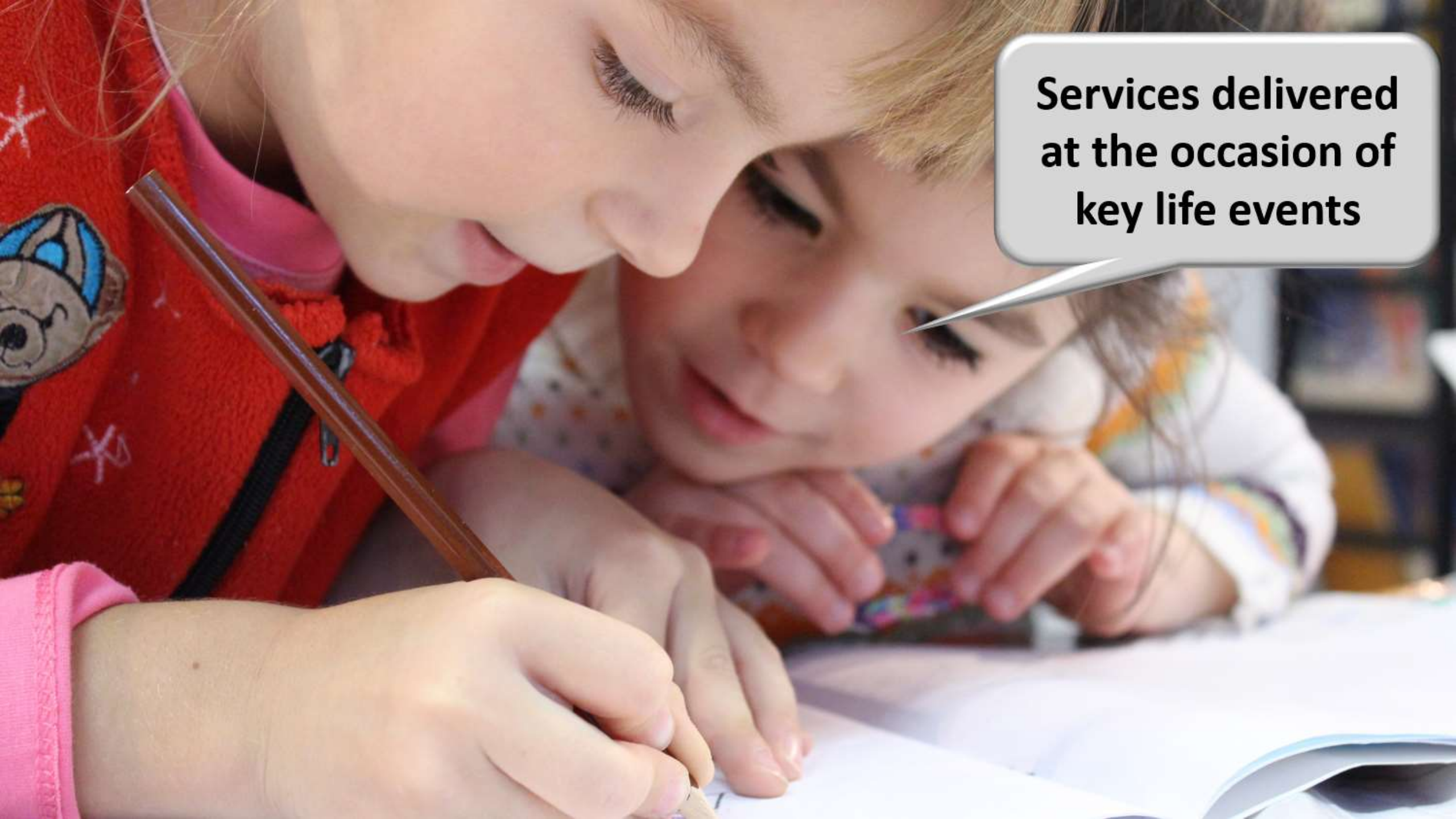

Question 1:
what do socially insured people, employers and policy makers expect ?


Effective social protection
Fraud prevention & repression
Policy support

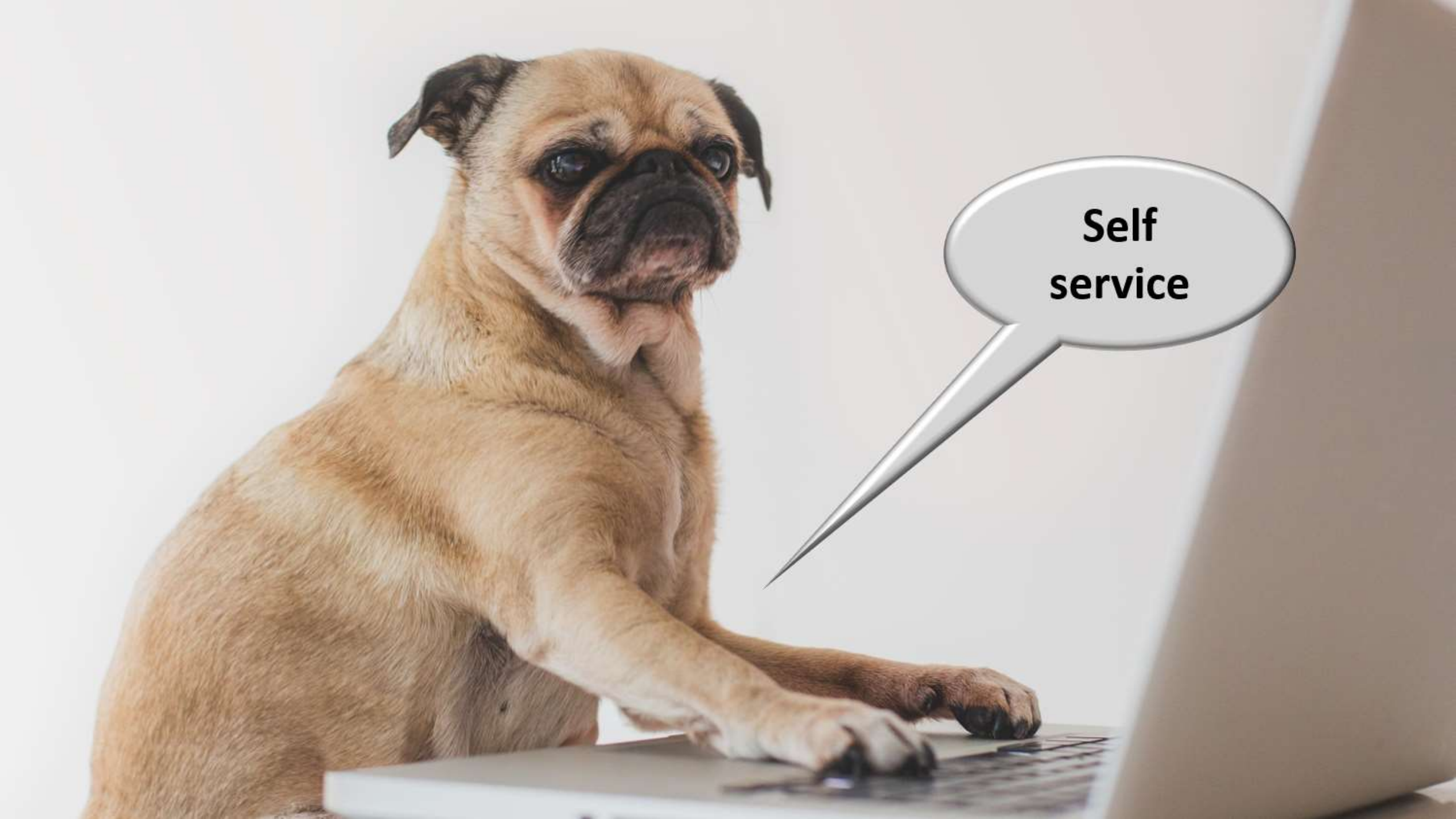

Benefits automatically granted
Happy flow


No digital divide
GO EGO LEGO
ZOMBIE LAND
BUS WAR OH
ALONE
THE END

Integrated services across institutions

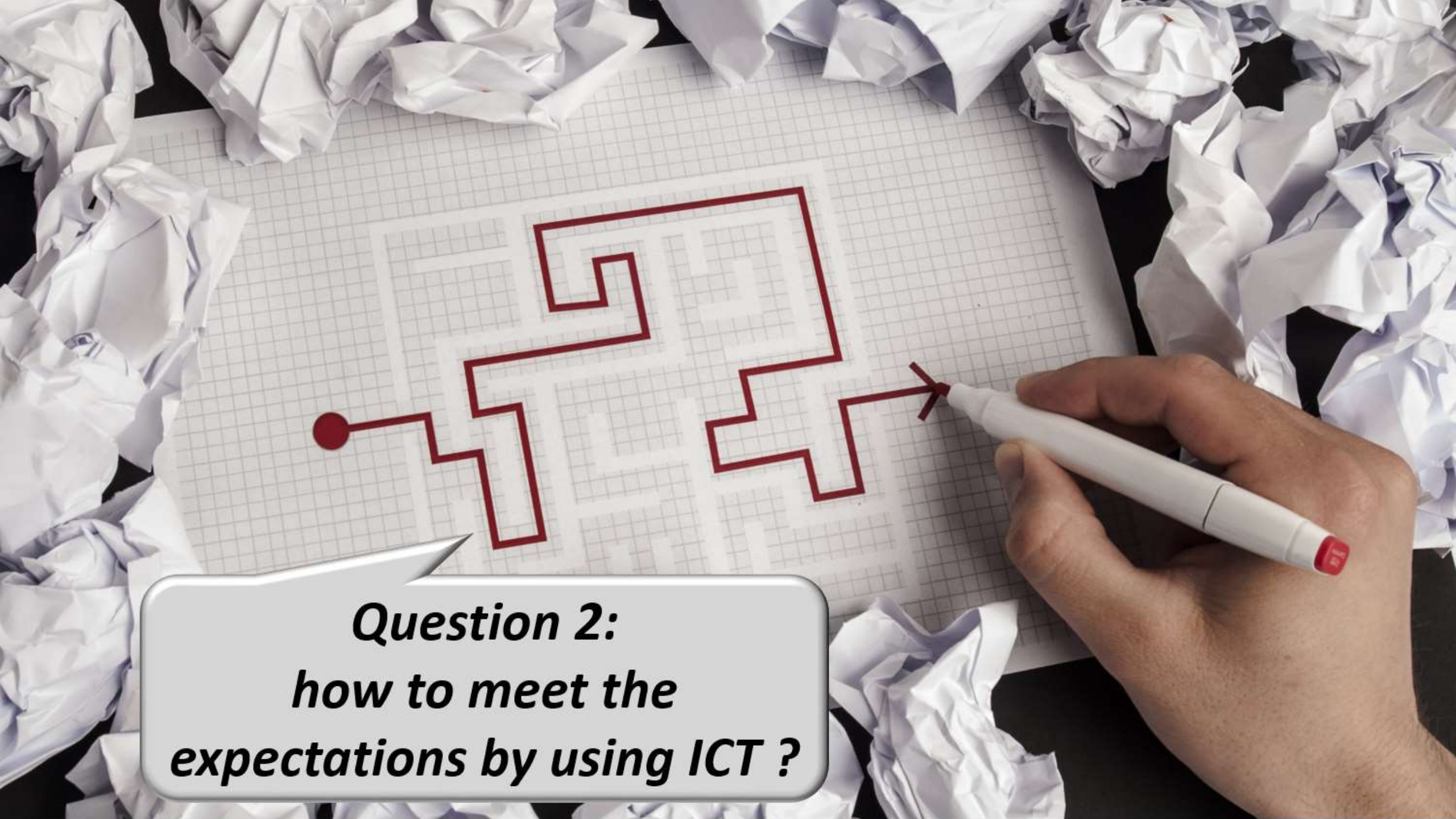

Services delivered at the occasion of key life events


Minimal administrative burden and minimal cost


Self
service


No
wrong
door


Fair competition
Legal certainty


Question 2:
how to meet the
expectations by using ICT ?


Common vision
Co-operation


Only once collection of factual data


Multifunctional
data use


Business process
re-engineering


Authentic sources & data sharing


Security: confidentiality, availability, integrity
Risk management via multilayered measures

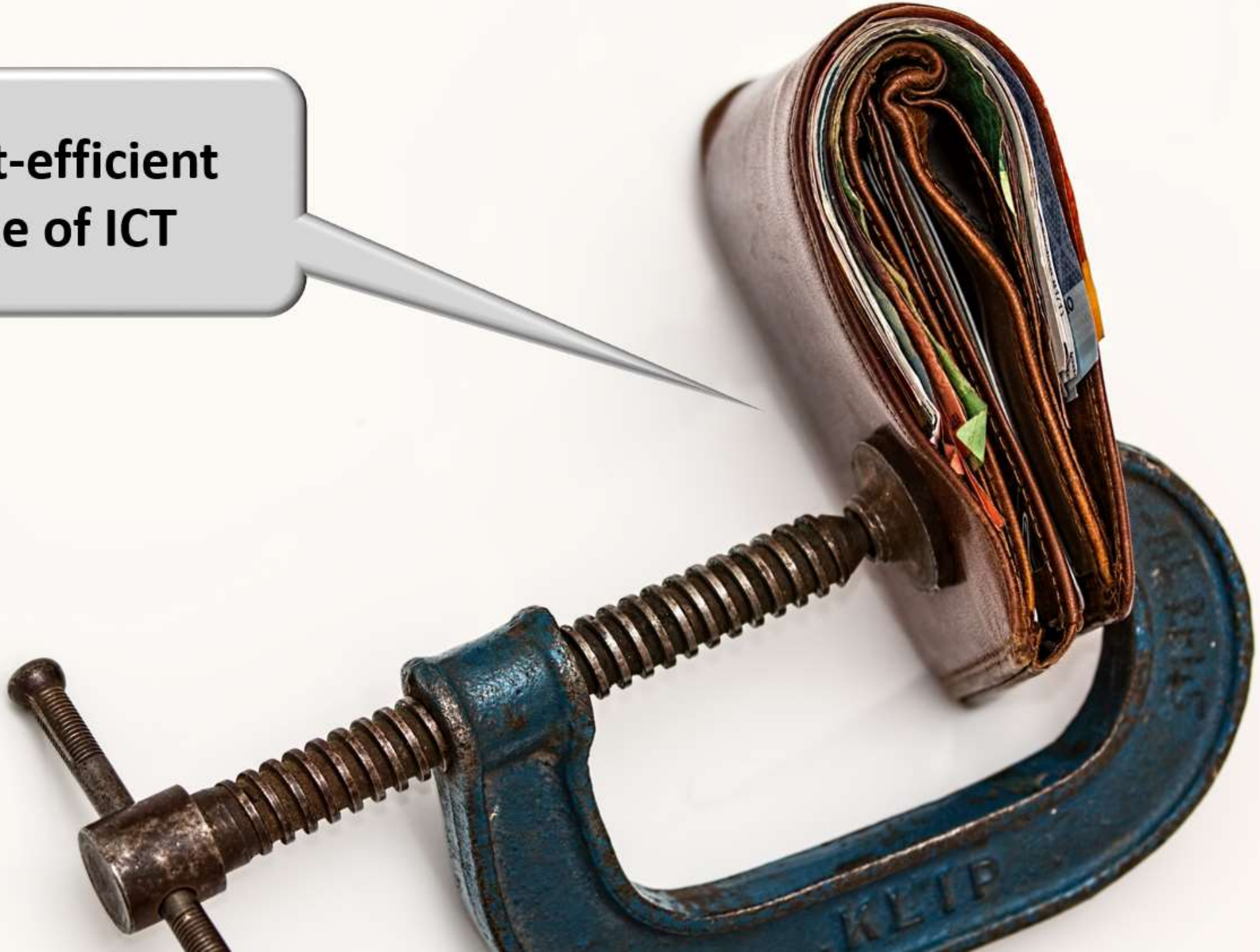

Access
authorization
& logging

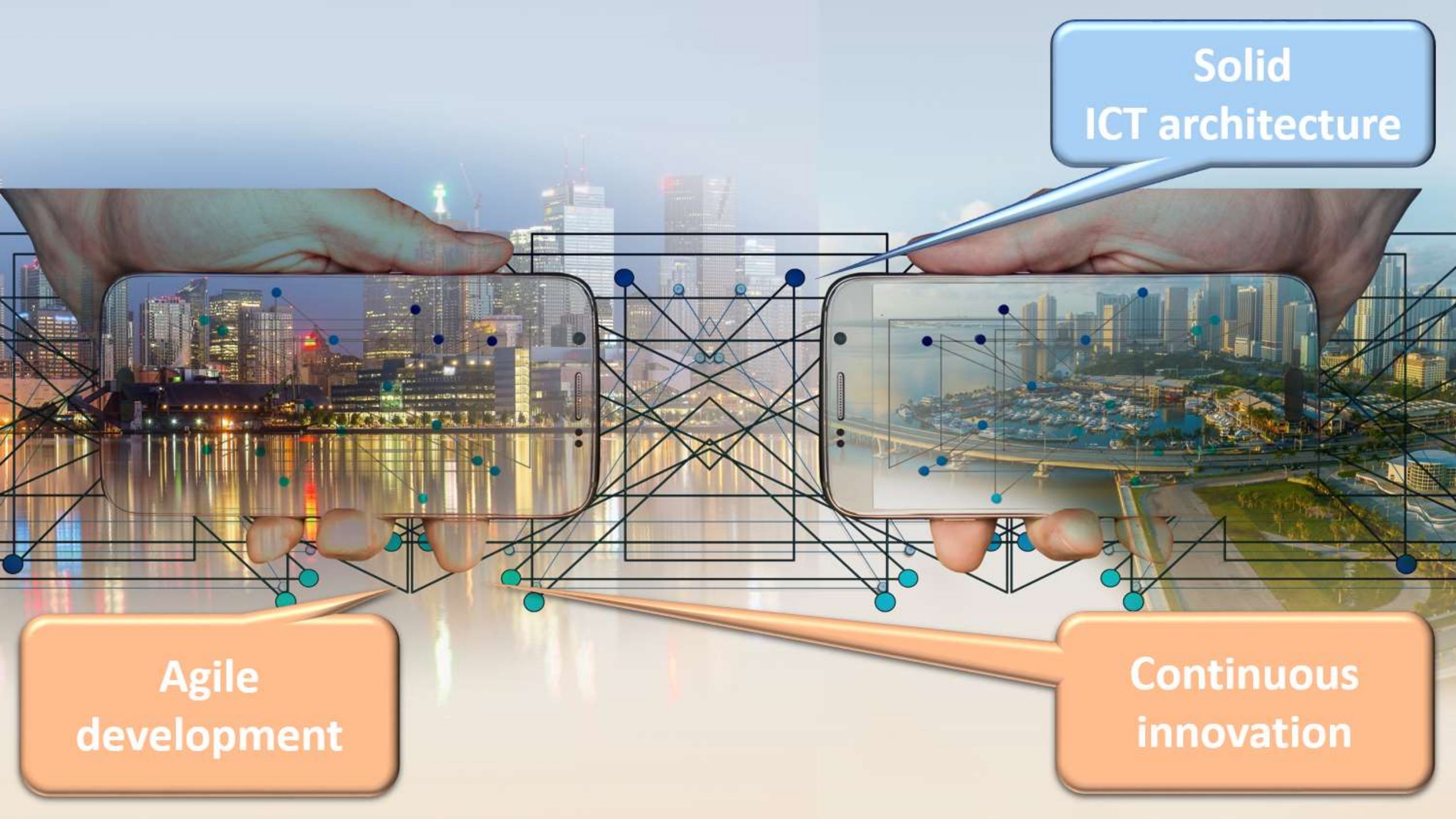

Computer literacy

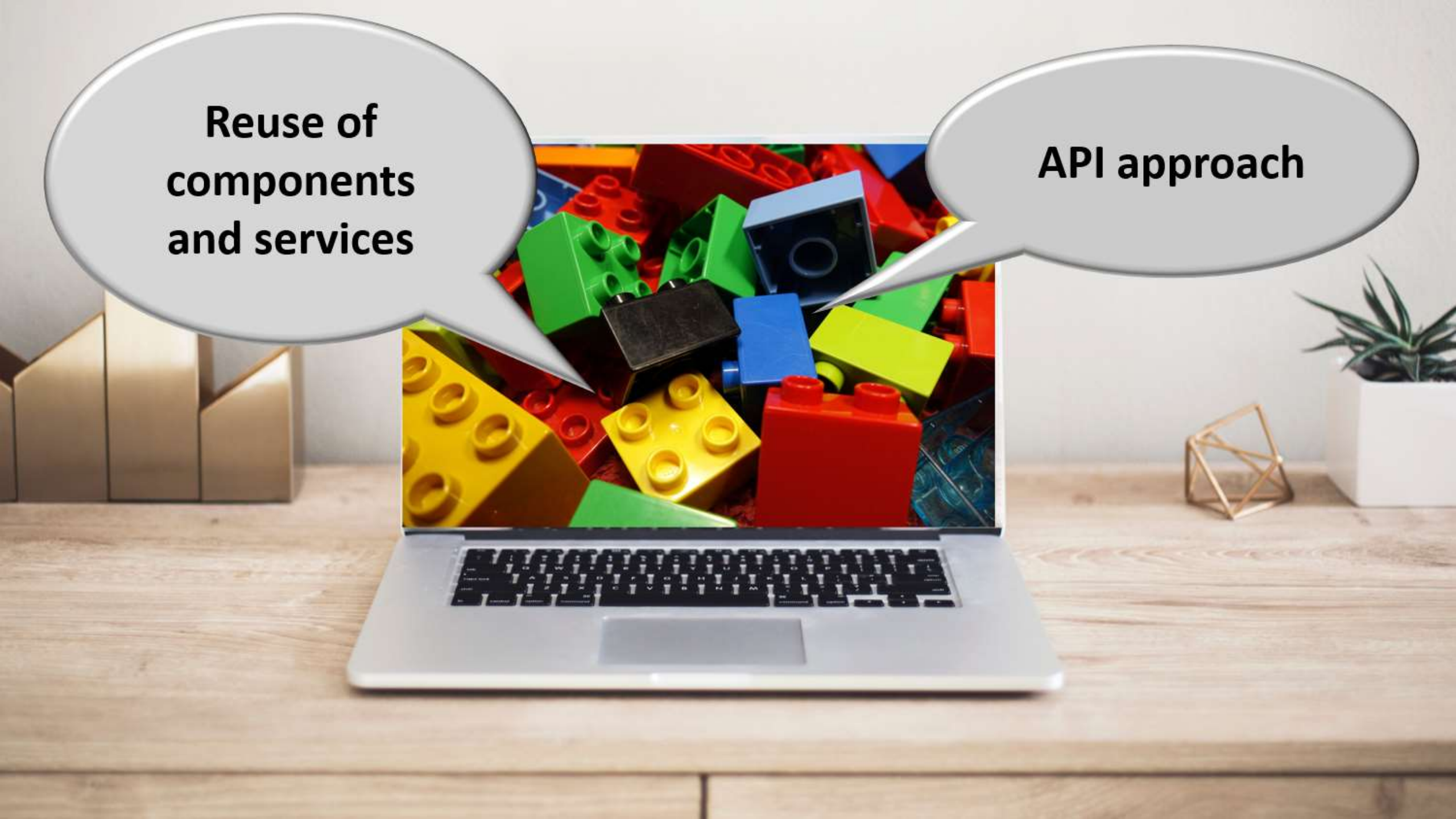

Entrepreneur-
ship
Corporate
culture and
teamwork


Added value rather than existing legal competences

Cost-efficient use of ICT




Solid
ICT architecture
Agile
development
Continuous
innovation


Reuse of components and services
API approach


Service Oriented Architecture (SOA)
REpresentional State Transfer (REST)
Plug & play


Technology
&
policy watch

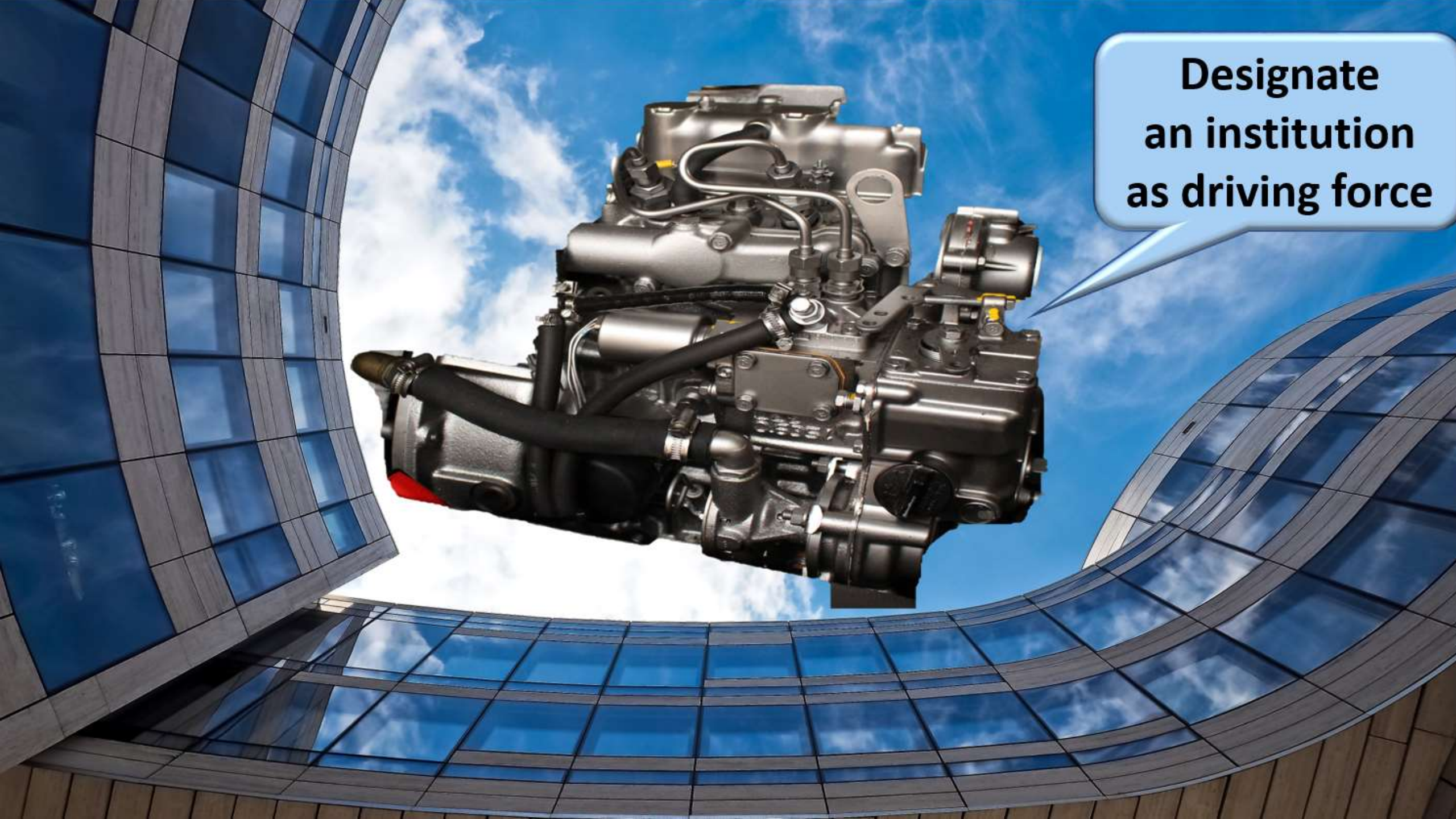

Mobile
applications


Cloud computing
• cost reduction
• faster time to market


Big data analysis for
• fraud prevention
• policy support
• detection of non-take up

Artificial intelligence

- support of big data analysis
- virtual personal assistants
- machine learning


Designate
an institution
as driving force


Human skills
Machine strength

Importance of good information management

Policy effectiveness

- information systems for
  - policy support
  - research
  - policy evaluation
- strategic use of information systems for
  - avoidance of non-take-up (automatic awarding)
  - social inclusion
  - fraud avoidance and control
  - continuity in granting rights
  - …

Efficiency of policy implementation

- operational excellence
- information management and information security
  - collected and validated once
  - correct and timely available
  - reusable and shared (authentic sources)
- processes
  - event-driven
  - process chains
  - division of tasks between actors in function of competence
- architecture
  - Service Oriented Architecture
  - modularity and encapsulation
  - synergies via cloud and container technology

Origins of the CBSS initiative

- stakeholders of the Belgian social sector
  - > 11,560,000 citizens
  - > 230,000 employers
  - about 3,000 public and private institutions (actors) at several levels (federal, regional, local) dealing with
    - collection of social security contributions
    - delivery of social security benefits
      - child benefits
      - unemployment benefits
      - benefits in case of incapacity for work
      - benefits for the disabled
      - re-imbursement of health care costs
      - holiday pay
      - old age pensions
      - guaranteed minimum income
    - delivery of supplementary social benefits
    - delivery of supplementary benefits based on the social security status of a person

Origins of the CBSS initiative

- a lack of well coordinated service delivery processes and of a lack of well coordinated information management led to
  - a huge avoidable administrative burden and related costs for
    - the citizens
    - the employers/companies
    - the actors in the social sector
  - service delivery that didn't meet the expectations of the citizens and the companies
  - suboptimal effectiveness of social protection
  - insufficient social inclusion
  - too high possibilities of fraud
  - suboptimal support of social policy
- at the same moment there were
  - a clear political will to solve those problems
  - a scientifically well-founded solution based on the creation of a Crossroads Bank stimulating and coordinating business process re-engineering and electronic co-operation

Common vision on information management

- information is being modelled
  - in such a way that the model fits in as closely as possible with the real world
  - in order to allow multifunctional use of information
- information is collected from citizens and companies only once by the social sector as a whole
  - via a channel chosen by the citizens and the companies
  - preferably from application to application
  - and with the possibility of quality control by the supplier before the transmission of the information
- the collected information is validated once
  - according to established task sharing criteria
  - by the actor that is most entitled to it or by the actor which has the greatest interest in correctly validating it

Common vision on information management

- a task sharing model is established indicating which actor stores which information as an authentic source, manages the information and maintains it at the disposal of the authorized users
- information can be flexibly assembled according to ever changing legal concepts
- every actor has to report probable errors of information to the actor that is designated to validate the information
- every actor that has to validate information according to the agreed task sharing model, has to examine the reported probable errors, to correct them when necessary and to communicate the correct information to every known interested actor
- once collected and validated, information is stored, managed and exchanged electronically to avoid transcribing and re-entering it manually

Common vision on information management

- electronic information exchange can be initiated by
  - the actor that disposes of information
  - the actor that needs information
  - the organisation that manages the interoperability framework
- electronic information exchanges take place on the base of a functional and technical interoperability framework that evolves permanently but gradually according to open market standards, and is independent from the methods of information exchange
- available information is used for
  - the automatic granting of benefits
  - prefilling when collecting information

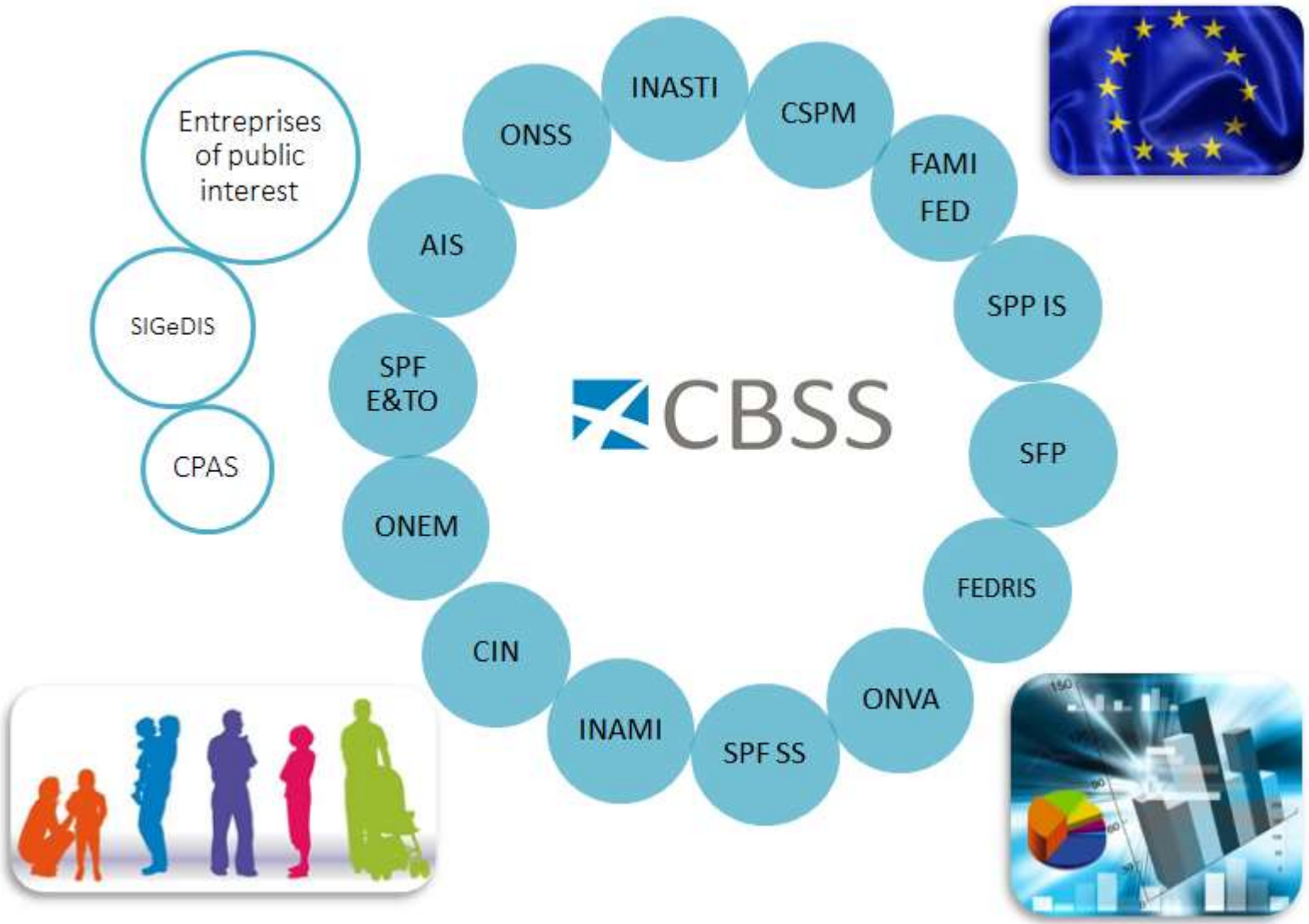
Common vision on information security

- security, availability, integrity and confidentiality of information is ensured by integrated structural, institutional, organizational, HR, technical and other security measures according to agreed policies
- personal information is only used for purposes compatible with the purposes of the collection of the information
- personal information is only accessible to authorized actors and users according to business needs, legislative or policy requirements
- the access authorization to personal information is granted by an Information Security Committee, designated by Parliament, after having checked whether the access conditions are met
- the access authorizations are public

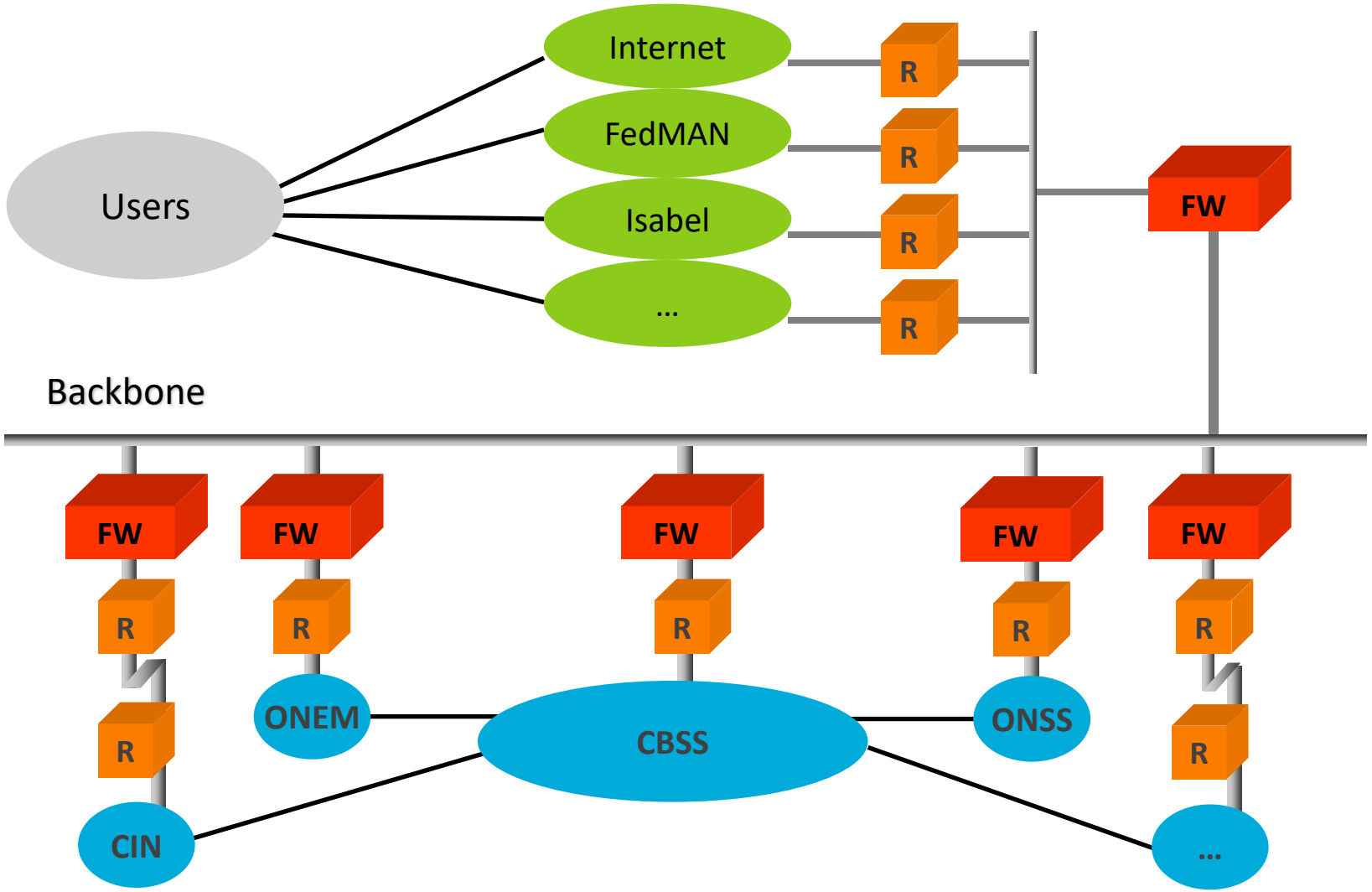
Common vision on information security

- every actual electronic exchange of personal information has to pass an independent trusted third party and is preventively checked on compliance with the existing access authorizations by that trusted third party
- every actual electronic exchange of personal information is logged, to be able to trace possible abuse afterwards
- every time information is used to take a decision, the information used is communicated to the person concerned together with the decision
- every person has right to access and correct his/her own personal data
- every actor in the social sector disposes of an information security officer with an advisory, stimulating, documentary and control task

The solution – the network



The solution – the network



The solution - Business Process Reengineering (BPC)

- first process optimisation, then computerization; otherwise risk to consolidate suboptimal processes

- building of integrated value chains through
  - mutual coordination between internal business processes and processes of suppliers, partners, customers, …
  - provision of basic and business services for integration into global applications, offered by third parties to end users

- importance of standardisation importance of involvement of users of processes (no wrong door)

The solution – concrete results and impact

- a network between all 3,000 social sector actors with a secure connection to the internet, the federal MAN, regional extranets, extranets between local authorities and the Belgian interbanking network

- a unique identification key
  - for every citizen
  - for every company
  - for every establishment of a company

- an agreed division of tasks between the actors within and outside the social sector with regard to collection, validation and management of information and with regard to electronic storage of information in authentic sources

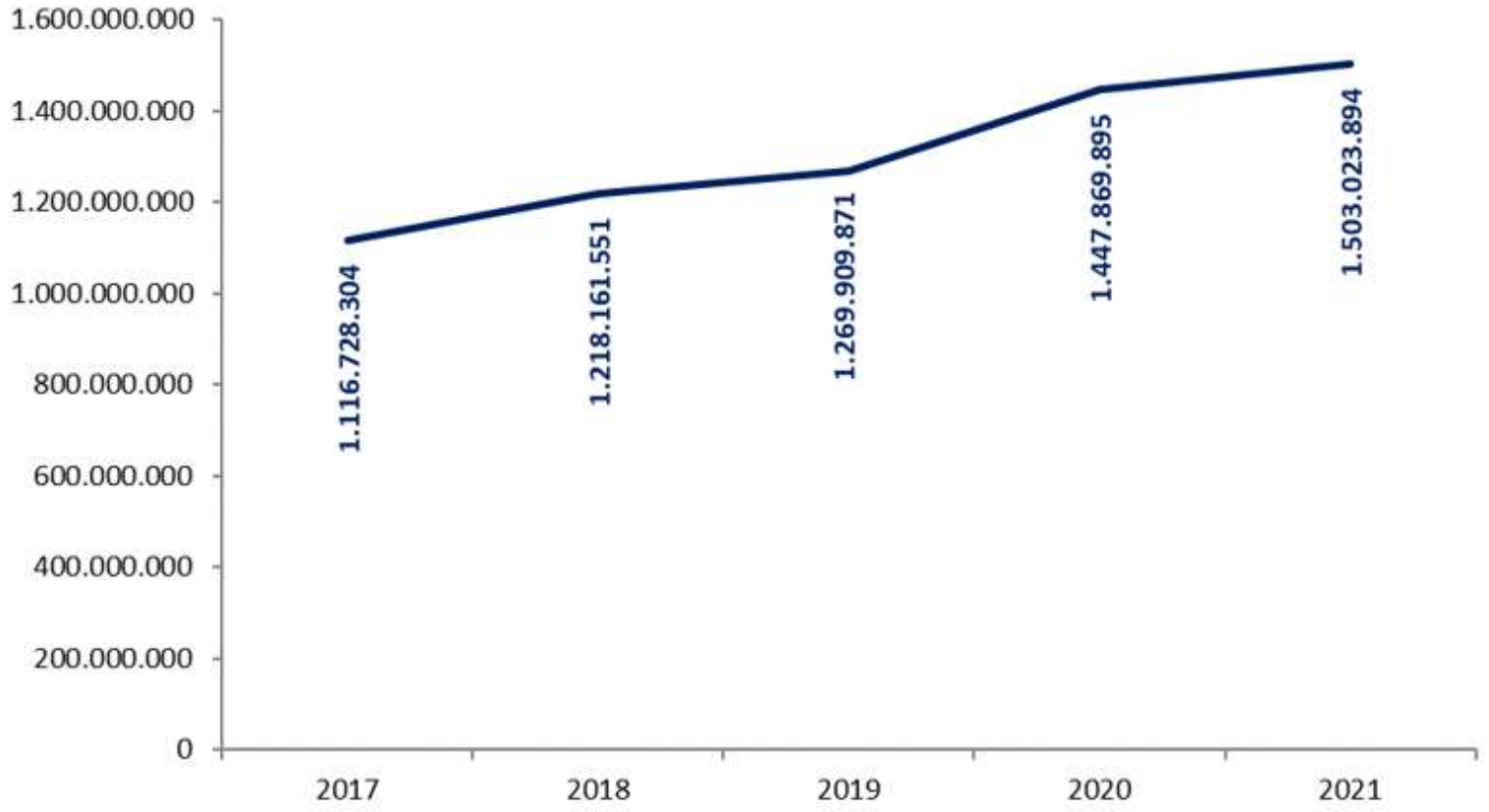
The solution – concrete results and impact

- 220 electronic services for mutual information exchange amongst actors in the social sector, defined after process optimization
  - nearly all direct or indirect (via citizens or companies) paper-based information exchange between actors in the social sector has been abolished
  - in 2021, > 1,5 billion electronic messages were exchanged amongst actors in the social sector, which saved as many paper exchanges

- electronic services for citizens
  - maximal automatic granting of benefits based on electronic information exchange between actors in the social sector
  - 24 electronic services via an integrated portal and/or mobile applications

The solution – concrete results and impact

1.503.023.894 electronic messages were exchanged in 2021



The solution – concrete results and impact

- more than 50 electronic services for employers, either based on the electronic exchange of structured messages or via an integrated portal site
  - 50 social security declaration forms for employers have been abolished
  - in the remaining 30 (electronic) declaration forms the number of headings has on average been reduced to a third of the previous number
  - declarations are limited to 3 events
    - immediate declaration of recruitment and discharge (only electronically)
    - quarterly declaration of salary and working time (only electronically)
    - occurrence of a social risk (electronically or on paper)
  - in 2021, more than 35 million electronic declarations were made by all 230,000 employers, 98 % of which from application to application

The solution – concrete results and impact

- an integrated portal site and mobile applications containing
  - electronic transactions for citizens, employers and professionals
  - simulation environments
  - information about the entire social security system
  - harmonized instructions and information model relating to all electronic transactions
  - a personal page for each citizen, each company and each professional
- an integrated multimodal contact centre supported by a customer relationship management tool
- a data warehouse containing statistical information with regard to the labour market and all branches of social security

Useful tool: the reference directory

- reference directory
  - directory of available services/information
    - which information/services are available at any actor depending on the capacity in which a person/company is registered at each actor
  - directory of authorized users and applications
    - list of users and applications
    - definition of authentication means and rules
    - definition of authorization profiles: which kind of information/service can be accessed, in what situation and for what period of time depending on in which capacity the person/company is registered with the actor that accesses the information/service
  - directory of data subjects
    - which persons/companies have personal files at which actors for which periods of time, and in which capacity they are registered
  - subscription table
    - which users/applications want to automatically receive what information/services in which situations for which persons/companies in which capacity

Useful tool: the electronic identity card

- identification of the holder
  - name
  - Christian names
  - nationality
  - date and place of birth
  - sex
  - identification number of the National Register
  - main residence
  - manual signature
- electronic authentication of the identity of the holder (private key and certificate)
- possibility for the holder to sign electronically (private key and certificate)
- no encryption certificate
- no electronic purse
- no biometric data

Integrated user and access management

Electronic identity card (eID): statutory electronic identity card for Belgians over the age of twelve

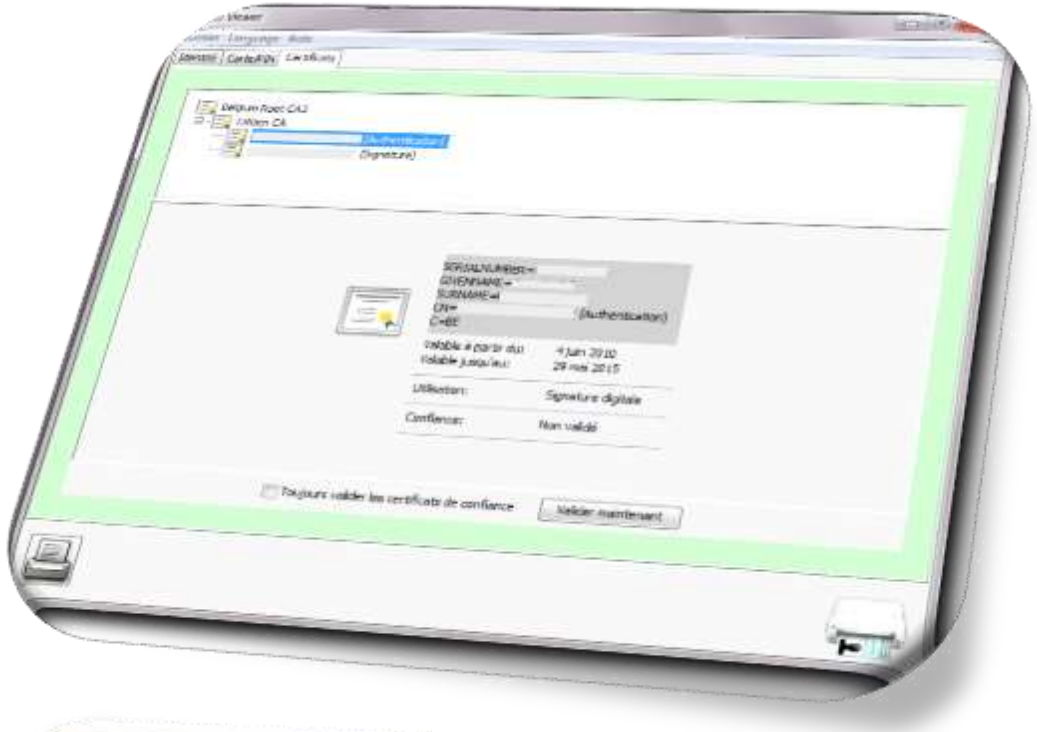
Kids-ID: on demand for children below the age of twelve

Foreigners card: for both EU and non-EU citizens with residence in Belgium

Electronic identity card (eID)

read data

authenticate identity



digital signatures

Electronic identity card (eID)

install eID software

connect the card reader with the computer

consult your data

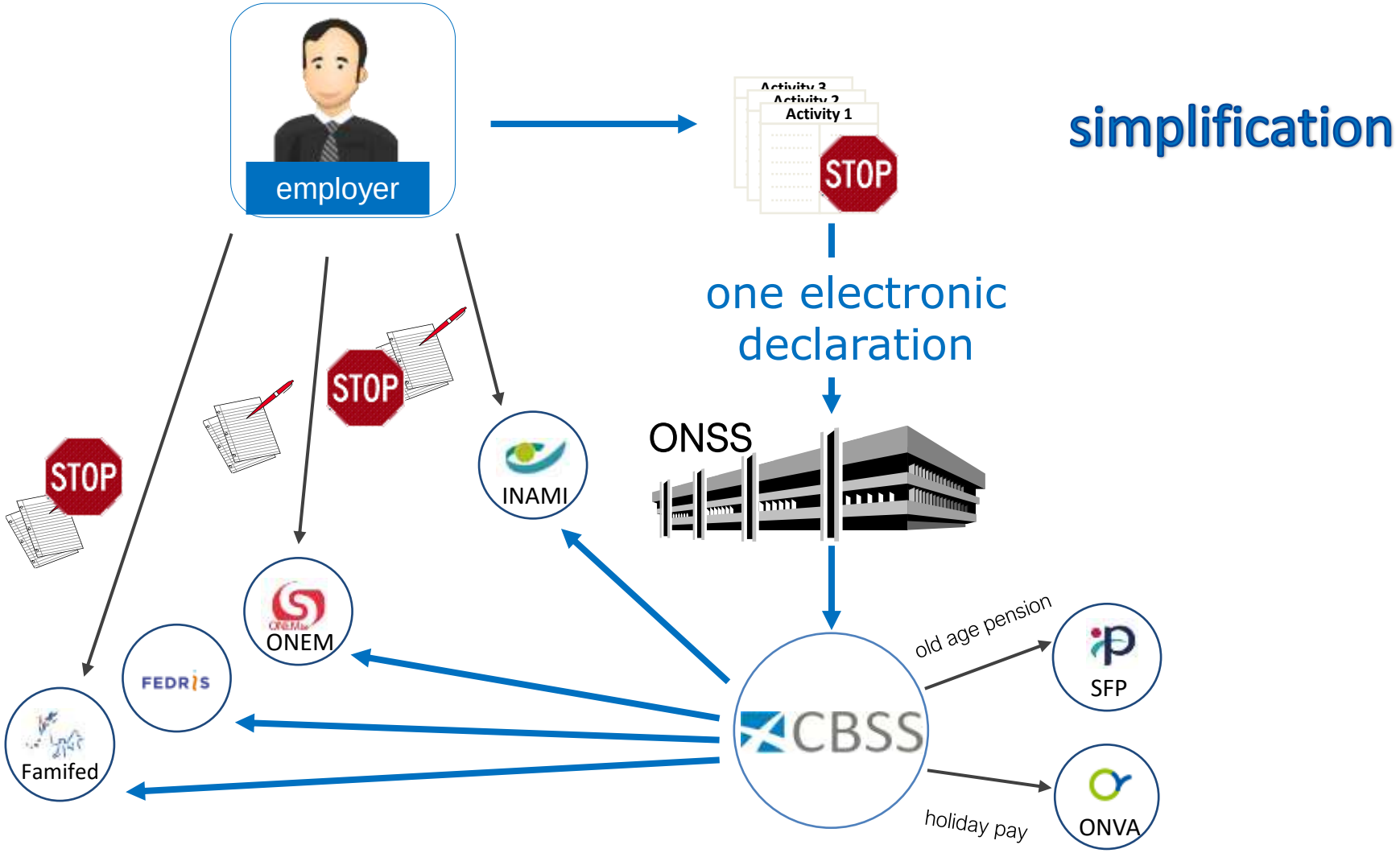
Distributed information servers

- information servers
  - directory of data subjects at the Crossroads Bank
  - basic identification data of citizens at the National Register and the complementary Crossroads Bank Register
  - basic identification data of companies at the Company Register
  - employers directory (WGR) at the ONSS
  - work force register at the ONSS
  - salary and working time database at the ONSS and the ONSSAPL
  - database of contribution certificates
- services offered
  - interactive consultation
  - batch consultation
  - automatic communication of updates

Pre-processed messages

- pre-processed messages
  - beginning/end of labour contract, beginning/end of self-employed activity
  - contribution certificates medical care (employees, self-employed, beneficiaries of social security allowances)
  - unemployment benefits
  - benefits in case of career break
  - benefits in case of incapacity for work ((labour) accident, (occupational) disease)
  - reimbursement of health care costs
  - child benefits
  - old age pensions
  - holiday pay
  - benefits for the disabled
  - guaranteed minimum income – social welfare
  - derived rights (e.g. tax reduction/exemption, free public transport, ...)
  - migrant workers
  - …
- services offered
  - interactive consultation
  - batch consultation
  - automatic communication of messages

Quartely declaration salary & working time



Declaration of social risks

- types of social risks
  - child benefits
  - incapacity for work ((labour) accident, (occupational) disease, …)
  - unemployment
  - old age pension
- 3 possible moments of declaration
  - start of the social risk
  - recurrence or continuation of the social risk
  - end of the social risk
- structure of the declaration
  - identification data
  - if necessary, salary and working time data not yet declared via a quarterly declaration (mini-declaration)
  - specific data concerning the social risk

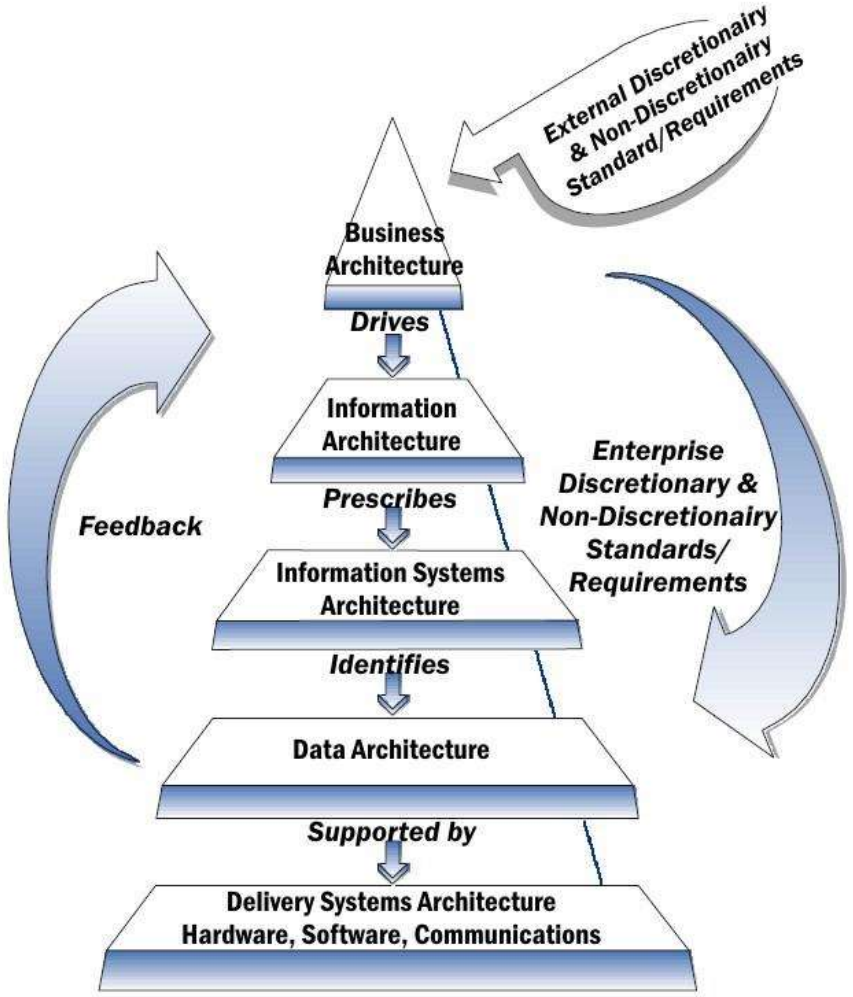
LIMOSA

- integrated electronic service delivery based on a single, mandatory declaration in case of temporary or partial professional activities of foreign employees and self-employed persons in Belgium
- 800.000 declarations per year
- reduction of process time from 7 days to 5 minutes
- integrated service throughout 8 types of institutions (750 concrete institutions)
- gains in effectiveness
  - improvement of social protection of migrant workers
  - enhancement of free movement of workers and services
- gains in efficiency
  - lower cost due to single, multifunctional and electronic information collection and integrated information processing
  - shortening of clearance times with immediate return of receipt
  - availability of integrated services according to the logic of the user at any time and from anywhere
- gains in transparency
  - permanent access for the user to the processing status of its declaration

Useful legislative changes

- legal translation of
  - the common vision on information management
  - the common vision on information security and privacy protection
  - the obligation to use unique identification keys
- creation of a public institution (CBSS) that acts as a driving force
  - mission and tasks
  - governance
  - financing principles
- creation of a control committee on information security and privacy protection
- probative value of electronic information storage and exchange
- punishment of abuse of the system
- gradually, coordination or harmonisation of basic legal concepts
- gradually, adaptation of business processes set out in the law

Architecture layers



- way to
  - understand how the information provision and ICT is structured and why
  - describe how the various components are built up and interlinked
  - control how this evolves over time
- goals
  - cost control: poor architecture and many changes increases costs exponentially
  - faster time to market
  - better maintainability
  - greater flexibility
  - greater mobility
  - greater security
  - higher availability of resources

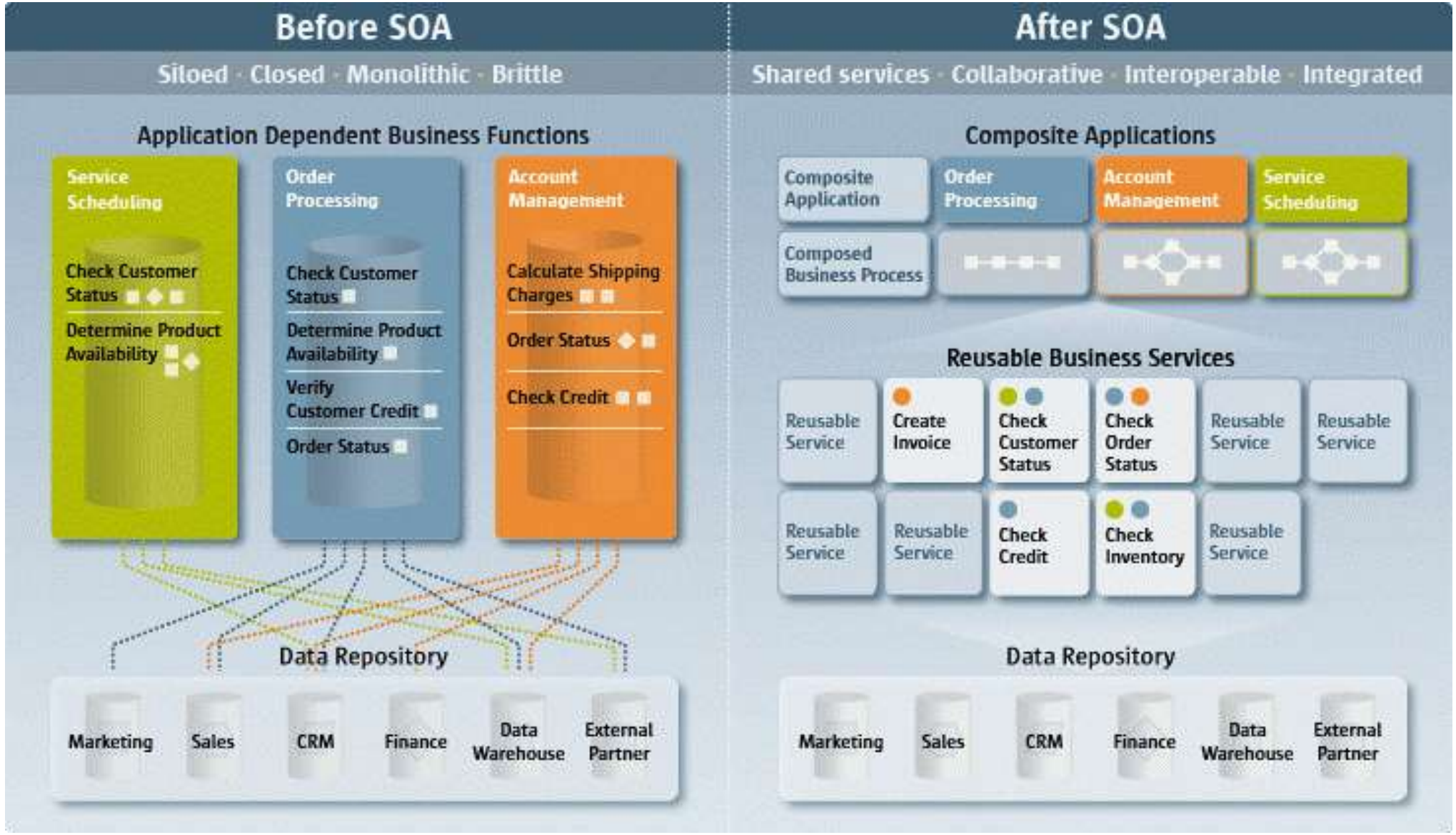
Service Oriented Architecture (SOA)

- what ?

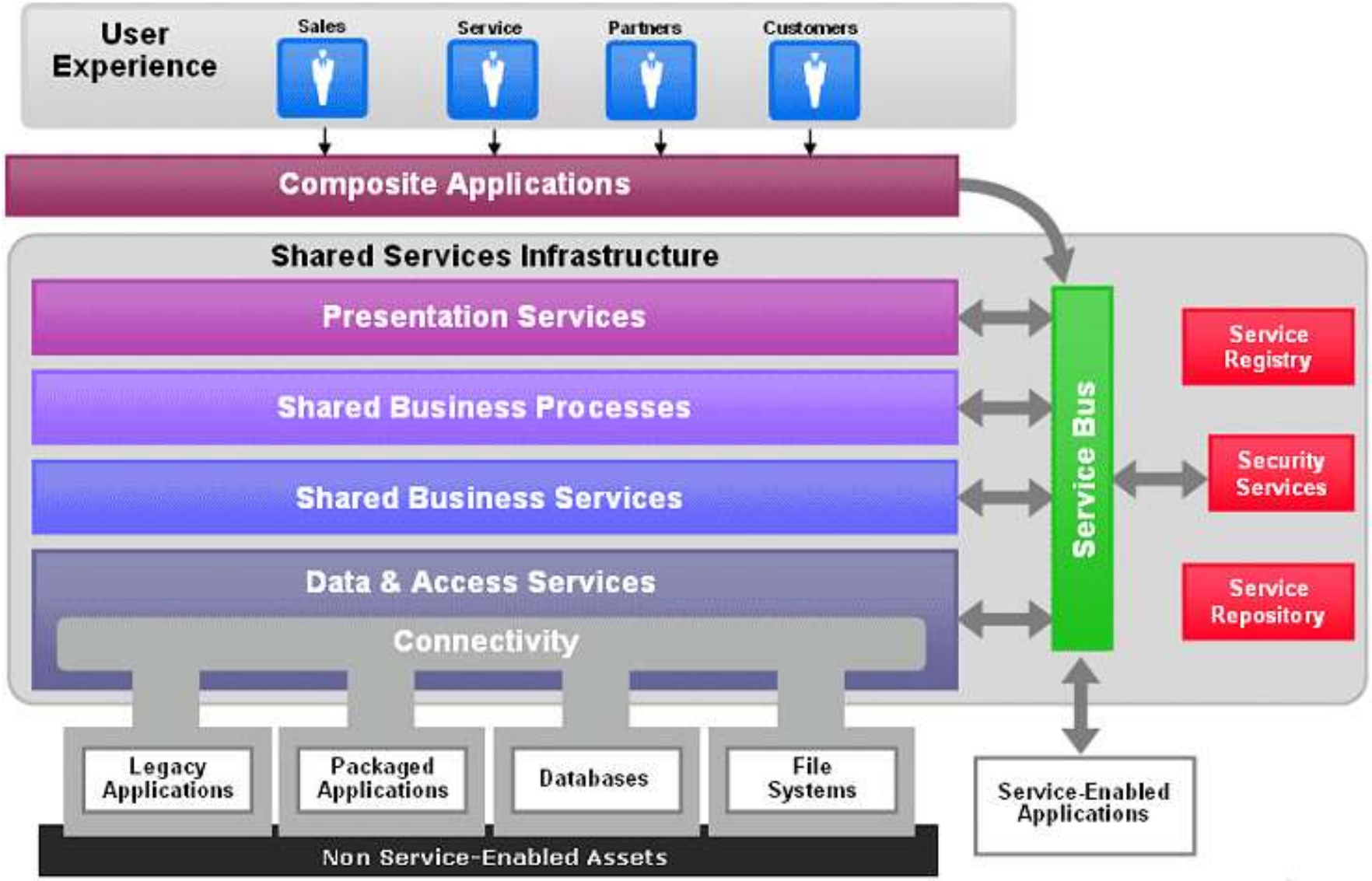
  “Service Oriented Architecture (SOA) is a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations. This style of architecture promotes reuse at the macro (service) level rather than micro levels (eg. objects). It also makes interconnection of existing IT assets trivial” (OASIS Reference Group)

- characteristics
  - service-oriented
  - modular
  - interoperable (based on open standards or open specifications)
  - extensible
  - layered
  - based on reuse of components and data

Service Oriented Architecture (SOA)

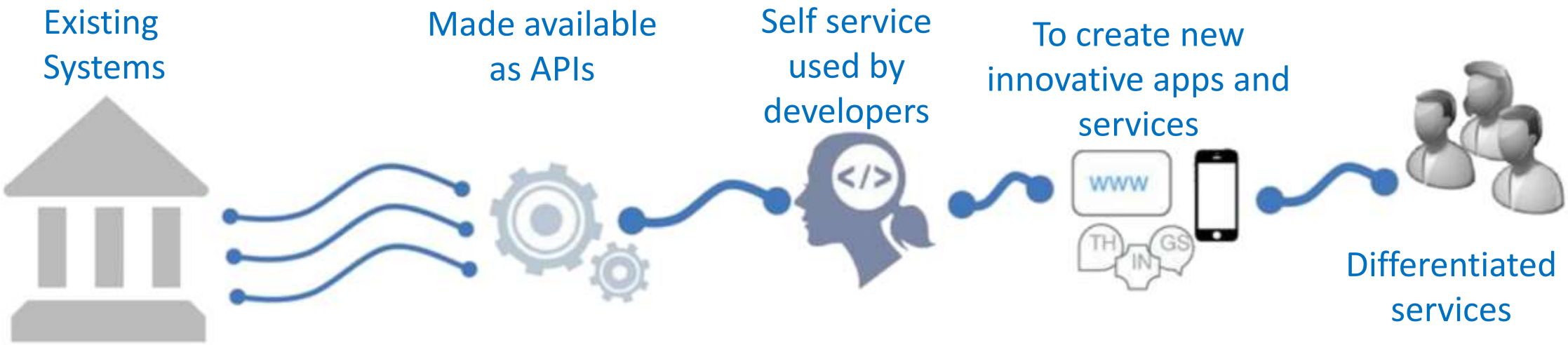


Service Oriented Architecture (SOA)



Shifting to an API economy: the value chain

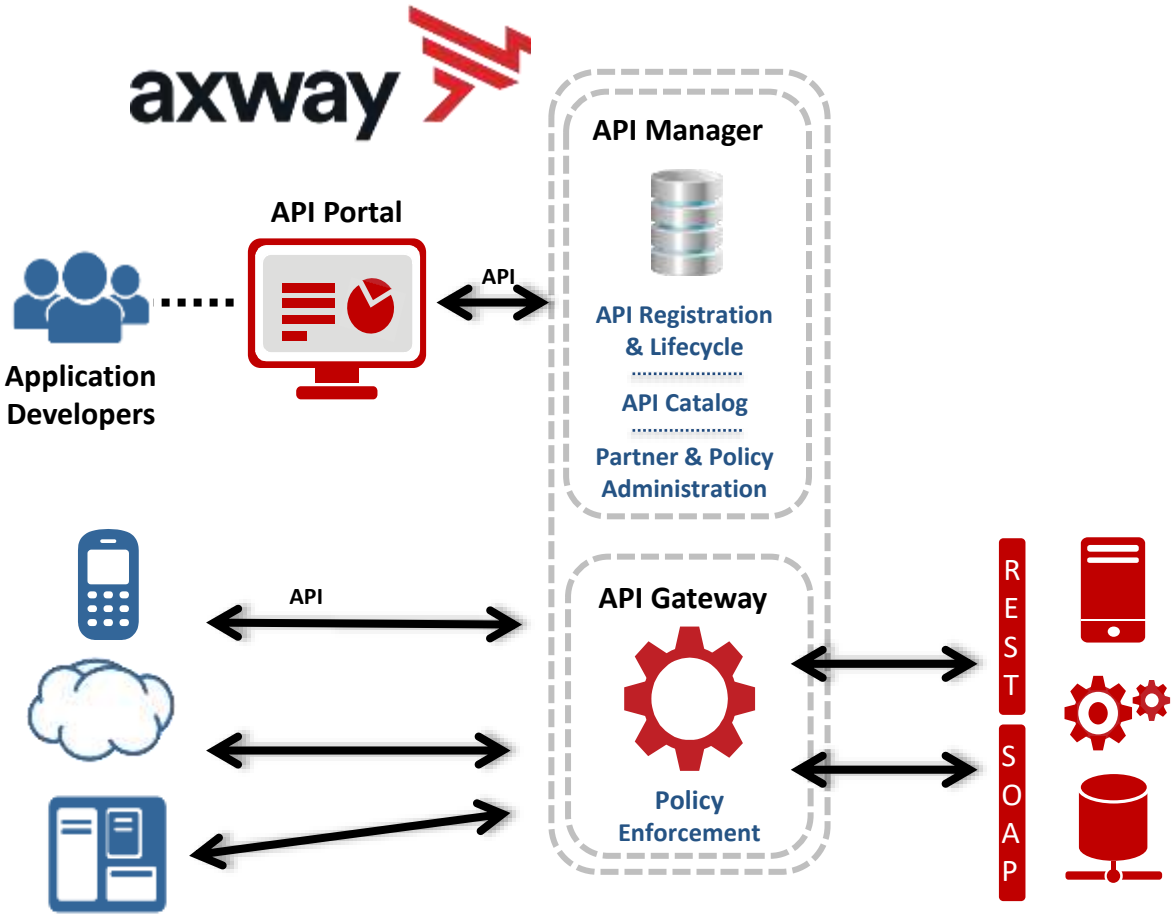
- API = Application Programming Interface
- APIs are key in real-time information exchange between software of several actors
- APIs drive today's business processes in eGovernment



Advantages of API approach

- cost reduction by reusability: consumers don’t need to rewrite what already exists!
- complexity reduction: no more big, monolithic systems
- decoupling: consumers and providers can continue to connect as long as the technical contract is followed → ex. less impact in case of migrations
- driver of innovation: new products raise, based on existing API capability
- stimulation of partnerships
- stimulation of standardization

API management solution



- from ESB-technology to API Gateway
  - parallel platform
  - zero-impact migration
- ready for today's technology, but supports our legacy as well
- flexible to extend and customize
- accelerates time-to-market

Beyond tooling: API management throughout the organization's soul

API Ecosystem eHeath
- ✓ 100+ APIs
- ✓ 1.200M transactions / month

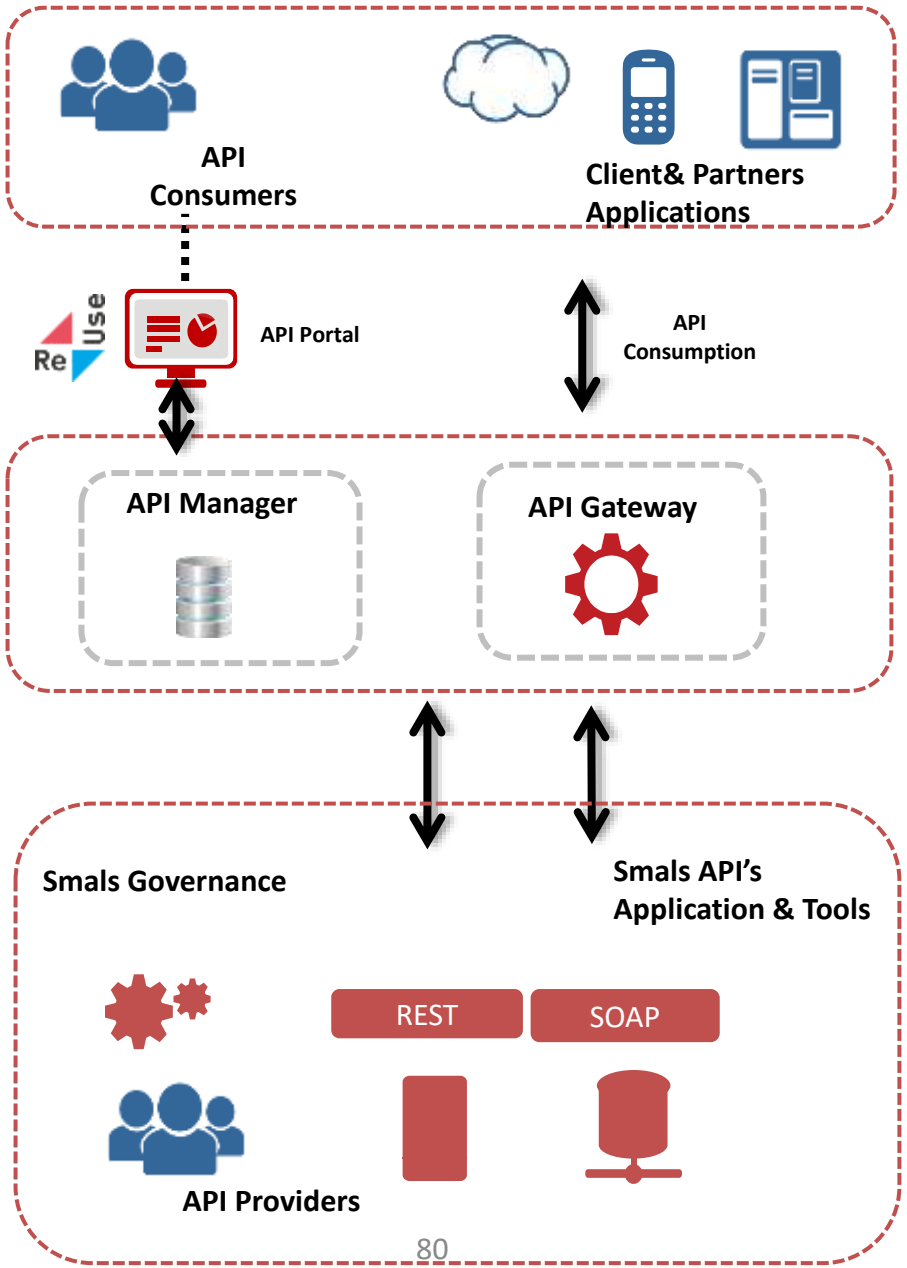
API Communication
- ✓ reUse Catalogue
- ✓ various Presentations

API Management
- ✓ API Catalogue

API Governance
- ✓ REST Board
- ✓ Integration Competency Center (ICC)

API Reporting
- ✓ API Metrics

API Operations
- ✓ Help Center



API Ecosystem Soc Sec
- ✓ 250+ APIs
- ✓ 600M transactions / month

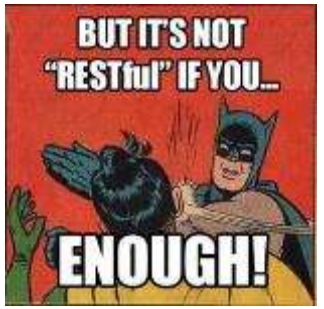
API Gateway
- ✓ tool API Gateway

API Architecture
- ✓ G-Cloud Platform is the reference

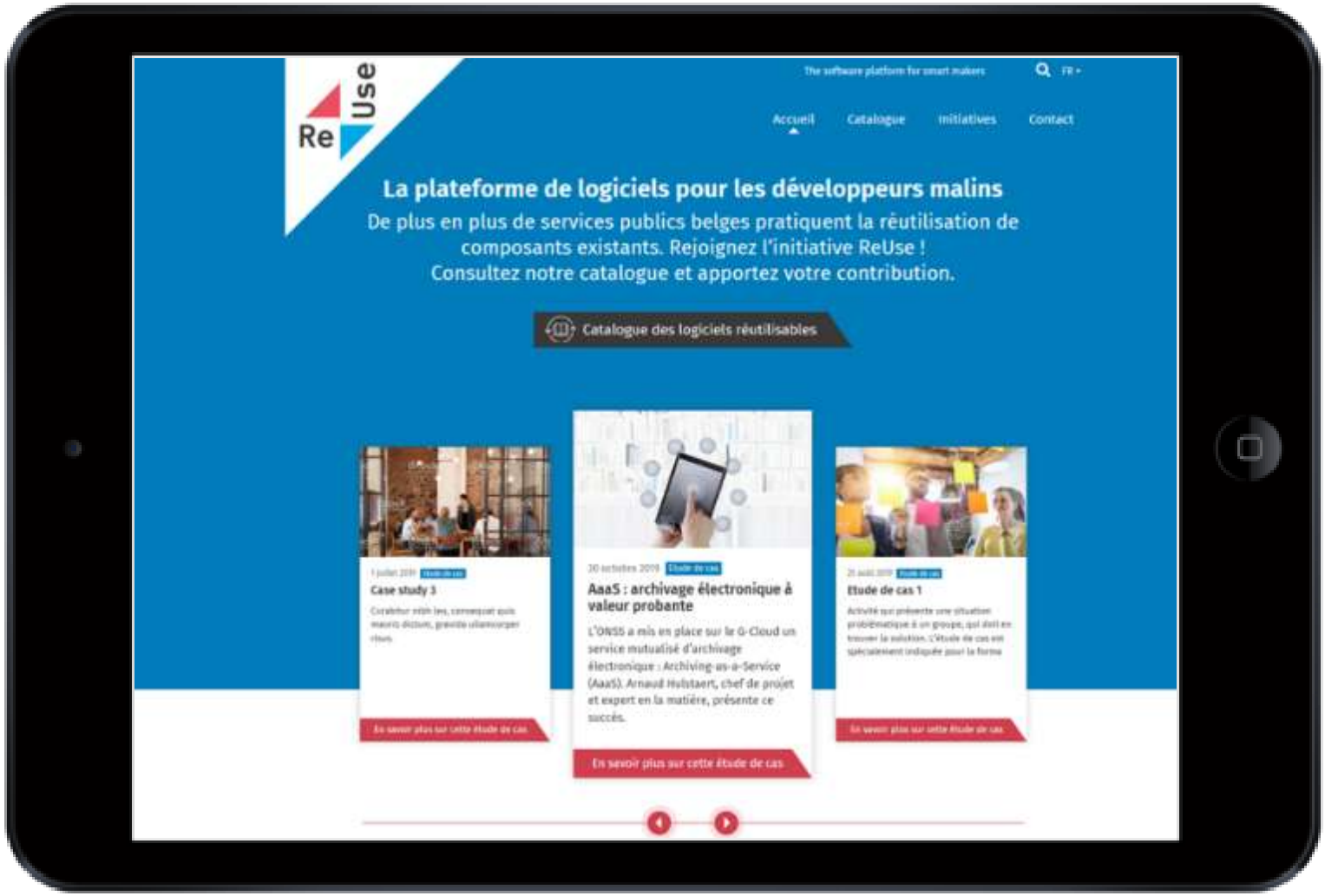
API Development
- ✓ development Guidelines
- ✓ API Trainings

G-Cloud REST style guide

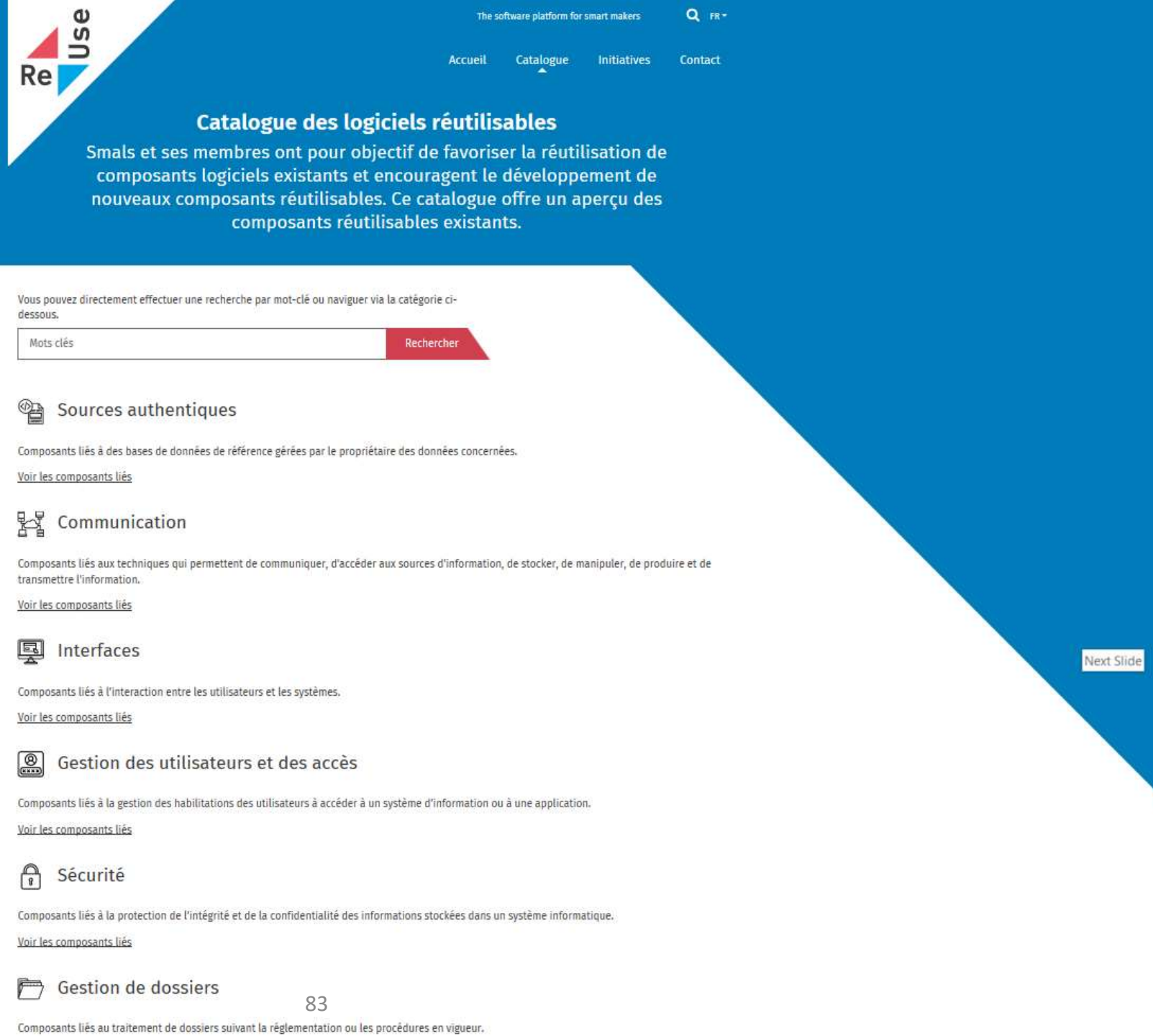
- based on industry standards and best practices
- a pragmatic approach to designing RESTful APIs
- collaborative effort organized in several workgroups:
  - REST API modelling
  - security (OAuth)
  - functional/business vocabularies (temporal, location, person, enterprises)
- work in progress
- https://www.gcloud.belgium.be/rest/



Software Reuse Platform: https://www.ict-reuse.be



New project?
consult the Software Reuse Catalogue



Next Slide

CBSS as driving force

- coordination by the Crossroads Bank for Social Security
  - Board of Directors consists of representatives of the companies, the citizens and the actors in the social sector
  - mission
    - definition of the vision and the strategy on eGovernment in the social sector
    - definition of the common principles related to information management, information security and privacy protection
    - definition, implementation and management of an interoperability framework
      - technical: secure messaging of several types of information (structured data, documents, images, metadata, …)
      - semantic: harmonization of concepts and co-ordination of necessary legal changes
      - business logic and orchestration support
    - coordination of business process reengineering
    - stimulation of service oriented applications
    - driving force of the necessary innovation and change
    - consultancy and coaching

Co-operative governance

- CBSS has an innovative model of governance, steering the business process re-engineering with complex interdependencies between all actors involved
- Board of Directors of the CBSS
  - consists of representatives of the stakeholders (employers associations, trade unions, social security institutions, …)
  - approves the strategic, operational and financial plans of the CBSS
- General Coordination Committee with representation of all users acts as debating platform for the elaboration and implementation of eGovernment initiatives within the social sector
- permanent or ad hoc working groups are instituted within the General Coordination Committee in order to co-ordinate the execution of programs and projects
- the chairmen of the various working groups meet regularly as a Steering Committee
- besides project planning and follow-up, proper measuring facilities are available to assure permanent monitoring and improvement after the implementation of the electronic services

Critical success factors and obstacles

- common vision on electronic service delivery, information management and information security amongst all stakeholders
- support of and access to policymakers at the highest level
- trust of all stakeholders, especially partners and intermediaries, based on
  - mutual respect
  - real mutual agreement
  - transparency
- respect for legal allocation of competences between actors
- co-operation between all actors concerned based on distribution of tasks rather than centralization of tasks
- focus on more efficient and effective service delivery and on cost control
- reasoning in terms of added value for citizens and companies rather than in terms of legal competences

Critical success factors and obstacles

- electronic service delivery as a structural reform process
  - process re-engineering within and across actors
  - back-office integration for unique information collection, re-use of information and automatic granting of benefits
  - integrated and personalized front-office service delivery
- multidisciplinary approach
  - business process optimization
  - legal coordination
  - ICT coordination
  - information security and privacy protection
  - change management
  - communication
  - coaching and training

Critical success factors and obstacles

- lateral thinking when needed
- appropriate balance between efficiency on the one hand and information security and privacy protection on the other
- quick wins combined with long term vision
- technical and semantic interoperability
- legal framework
- adaptability to an ever changing societal and legal environment
- creation of an institution that stimulates, co-ordinates and assures a sound program and project management

Critical success factors and obstacles

- availability of skills and knowledge => creation of an association that hires ICT-specialists at normal market conditions and puts them at the disposal of the actors in the social sector
- sufficient financial means for innovation: agreed possibility to re-invest efficiency gains in innovation
- service oriented architecture (SOA)
- need for radical cultural change within government, e.g.
  - from hierarchy to participation and team work
  - meeting the needs of the customer, not the government
  - empowering rather than serving
  - rewarding entrepreneurship within government
  - ex post evaluation on output, not ex ante control of every input

Advantages

- gains in efficiency
  - in terms of cost: services are delivered at a lower total cost
    - due to
      - a unique information collection using a common information model and administrative instructions
      - a lesser need to re-encoding of information by stimulating electronic information exchange
      - a drastic reduction of the number of contacts between actors in the social sector on the one hand and companies or citizens on the other
      - a functional task sharing concerning information management, information validation and application development
      - a minimal administrative burden
    - according to a study of the Belgian Planning Bureau, rationalization of the information exchange processes between the employers and the social sector implies an annual saving of administrative costs of about 1.7 billion € a year for the companies

Advantages

- gains in efficiency
  - in terms of quantity: more services are delivered
    - services are available at any time, from anywhere and from several devices
    - services are delivered in an integrated way according to the logic of the customer
  - in terms of speed: the services are delivered in less time
    - benefits can be allocated quicker because information is available faster
    - waiting and travel time is reduced
    - companies and citizens can directly interact with the competent actors in the social sector with real time feedback

Advantages

- gains in effectiveness: better social protection
  - in terms of quality: same services at same total cost in same time, but to a higher quality standard
  - in terms of type of services: new types of services, e.g.
    - push system: automated granting of benefits
    - active search of non-take-up using data warehousing techniques
    - controlled management of own personal information
    - personalized simulation environments
- better support of social policy
- more efficient combating of fraud

frank.robben@mail.fgov.be

@FrRobben

https://www.frankrobben.be
https://www.ksz.fgov.be
https://www.ehealth.fgov.be

Additional information

Belgian Crossroads Bank for Social Security

Implementation order used in Belgium

- common vision on information management and information security
- demonstration of feasibility
- political and public support, support of the social partners, support of the social security institutions
- basic legislation
  - creating an institution as a driving force and a control committee
  - translating the common vision on information management and information security
- integration of unique identification key in all information systems
- implementation of the ICT architecture and the basic ICT services
- controlled access to databases with authentic data
- re-engineering of processes between actors in the social sector at all government levels
- re-engineering of processes between actors in the social sector and companies
- re-engineering of processes between actors in the social sector and citizens
- always combined with the necessary legislative changes

Gaining support

- a clear long term vision combined with quick wins
- federal Minister of Social Affairs as a political sponsor
- demonstration of organisational and technical feasibility
- gradual implication of
  - the general managers of all public social security institutions
  - the social partners managing the public social security institutions
  - the general managers of the private social security institutions
- successive formal approval of the vision and the initiative by
  - all federal Ministers dealing with aspects of social security
  - the federal Council of Ministers
  - the National Labour Council (highest consultative body between the government and the social partners)
  - the federal Parliament

Gaining support

- small team in direct support of the federal Minister of Social Affairs
  - consisting of
    - experienced civil servants with a sound human network within all levels of the social sector
    - scientific experts
    - political advisors
  - with multidisciplinary skills
    - business process re-engineering
    - change management
    - legal
    - ICT
    - information security and privacy protection
    - communication
    - program and project management
- gradually, co-operation agreements with other government levels (regions, local authorities, …)

Institutional structure & financing of the CBSS

- cooperative governance
- adequate management and control techniques
- financing principles
- internal organization

Management and control techniques

- annual priority plan debated with all users within the General Coordination Committee of the CBSS

- cost accounting and zero-based budgeting resulting in financial transparency, an informed budget and a good evaluation of the management contract with the Belgian federal government

- internal control based on the COSO-methodology (see www.coso.org) in order to provide reasonable assurance regarding the achievement of objectives with regard to
  - effectiveness and efficiency of operations
  - reliability of financial reporting
  - compliance with applicable laws and regulations

- external audit with regard to the correct functioning of the internal control system

Management and control techniques

- program management through the whole social sector
- issue management during the management of each program
- use of a system of project management combined with a time keeping system to follow up projects that are realized by the CBSS and its partners
- frequent reports to all users which describe the progress of the various projects and eventual adjustment measures
- use of balanced scorecards and a dashboard to measure, follow-up and evaluate the performance of the electronic services and the CBSS
- use of ITIL (see www.itil-itsm-world.com) for ICT-service delivery
- use of a coherent set of monitoring techniques to guarantee an optimal control and transparency of the electronic services

Financing principles

- annual cost of the CBSS, its network and its services: 17.500.000 euro
- financed by a withholding on the social security contributions paid by the employers, the employees and the self-employed before the distribution of these contributions to the social security sectors
- no direct charge for the actors in the social sector in case of use of the CBSS services
  - stimulation of the use of the system
  - no additional accounting and administration costs for the social sector as a whole
- charge per electronic message (0,0055 euro) exchanged for actors outside the social sector, with possibility of settlement on mutual terms in case of reciprocal information exchange

Internal organization CBSS

- internal
  - 90 people
  - General Management
  - 6 divisions
    - R&D, Legal and External Communication
    - Client, Program, Project and Services Management
    - Application Development and Management
    - ICT Management
    - Information Security and Internal Audit
    - Resources Management (HR, finance, logistics, …)
- co-sourced with association owned by the public social security institutions
  - physical network
  - some basic services (e.g. portal, contact centre, …)

Electronic Exchange of Social Security Information (EESSI)

EESSI

- IT system that helps social security institutions across the EU exchange information related to different branches like
  - sickness, maternity and equivalent paternity benefits
  - family benefits
  - benefits in respect of accidents at work and occupational diseases
  - unemployment benefits
  - old-age pensions, pre-retirement and invalidity benefits
  - survivor’s benefits and death grants
  - applicable legislation
- more rapidly and securely
- as required by the EU rules on social security coordination

EESSI

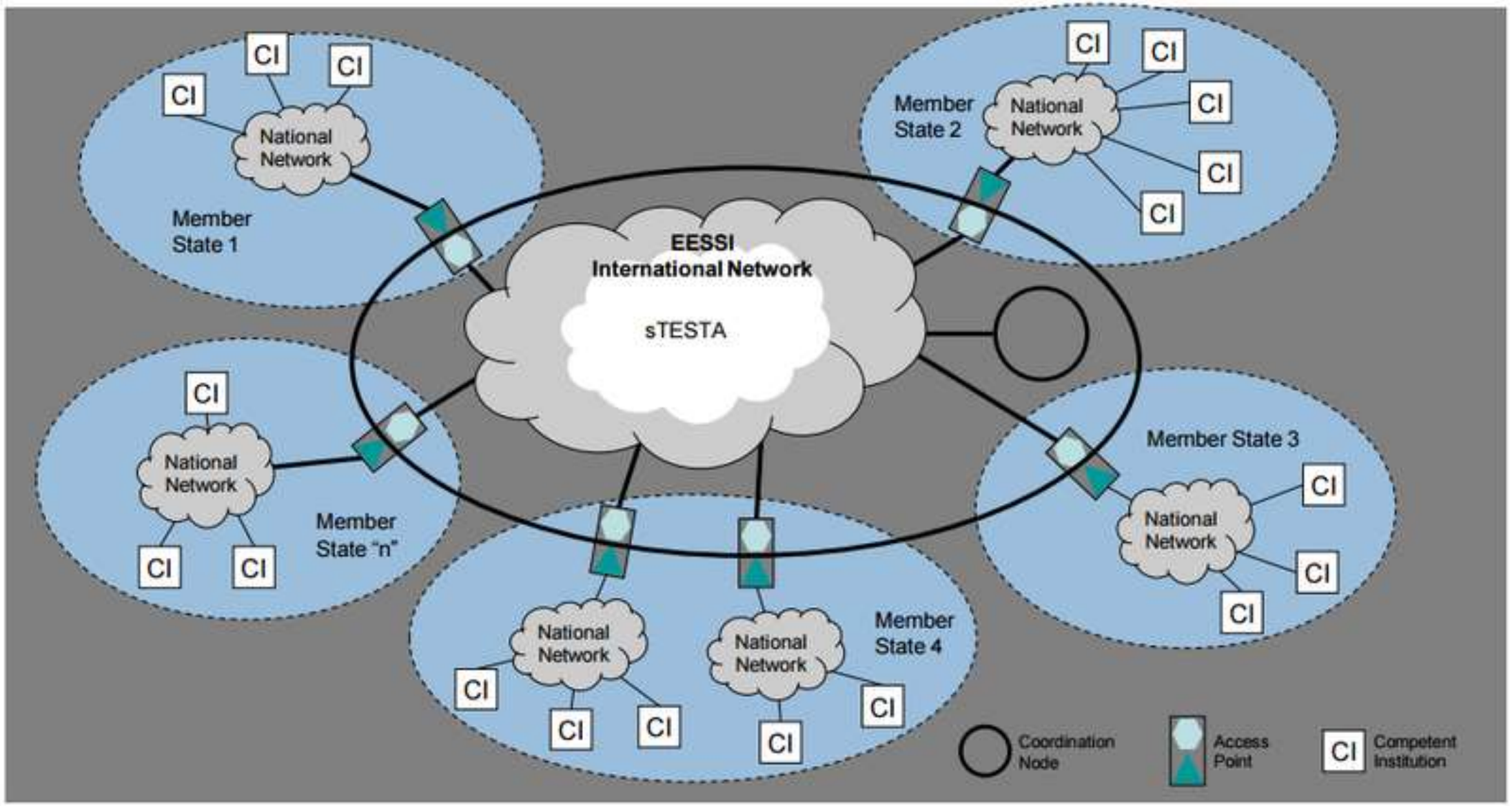
- all communication between national institutions on social security files are to take place through EESSI
- social security institutions exchange structured electronic documents and follow commonly agreed procedures to process them
- these documents are routed through EESSI to the correct destination in the right institutions in another Member State
- staff in social security institutions are able to find the correct destination in participating countries by consulting a repository of national institutions (see https://ec.europa.eu/social/social-security-directory/pai/pai/select-country/language/en)

EESSI

- 32 participating countries
  - 27 EU Member States
  - Iceland
  - Liechtenstein
  - Norway
  - United Kingdom
  - Switzerland

- > 5.000 participating institutions

EESSI architecture



EESSI architecture

- 135 Business Use Cases (BUCs), eg family benefits
  - FB BUC 01 – Determining competences
  - FB BUC 02 – Discharge of Family Benefits
  - FB BUC 03 – Additional Family Benefits for orphans
  - FB BUC 04 – Information about payment regarding priority right
- 276 Structured Electronic Documents (SED), eg FB BUC 03
  - F018 – request for insurance length period of additional benefits
  - F019 – reply for insurance length period of additional benefits
  - F020 – information on priority for additional benefits
  - F021 – application for additional benefits
- complete overview on https://www.frankrobben.be/wp-content/uploads/2022/04/EESSI-List-of-BUCs-SEDs.xlsx

EESSI type of data exchanged

- identification (name, unique identification number, …)
- basic attributes of a person (date/place of birth/death, gender, nationality, …)
- address
- bank account number
- civil status and family composition
- professional relations
- working regime
- working periods and assimilated periods
- income
- circumstances of occurance of a social risk
- competent social security institutions

Benefits of EESSI

- quicker and more efficient processing of social security benefits
- more correct and complete data and case handling thanks to standard electronic forms and procedures
- more efficient implementation of social security coordination rules
- social security institutions across the EU use standardised electronic documents translated into their own language, improving multilingual communication

Benefits of EESSI

- combating fraud and error
- secure handling of personal data
- enabling statistics on the message exchanges between social security institutions
- social security institutions across Europe can exchange relevant information also to verify the social security rights of mobile citizens

Security: confidentiality, availability, integrity

Global vision

- modern technologies can bring enormous benefits and added value, but they must be deployed with the right safeguards for the fundamental right to data protection
- international treaties and national constitutions provide for a whole series of fundamental rights: in addition to the right to data protection, there is also the right to a fair trial, the right to social protection, the right to high-quality healthcare, ...
- citizens can expect the government to ensure their right to data protection in a way that also respects their other fundamental rights
- possible drawbacks should be avoided, but benefits should not be unnecessarily obstructed
- risk management and data protection-by-design and a multidisciplinary approach are key concepts in this

Holistic approach

- legal framework
- minimal information security standards
- structural and institutional measures
- organisational measures
- technical measures

Legal framework: General Data Protection Regulation (GDPR)

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

- directly applicable without the need for transposition into national law

- applicable as from 25 May 2018

- see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

Basic principles GDPR (article 5)

Personal data shall be

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘**lawfulness, fairness and transparency**’)
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘**purpose limitation**’)
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation**’)
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘**accuracy**’)

Basic principles GDPR (article 5)

Personal data shall be

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘**storage limitation**’)
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality**’)

Lawfullness of processing (article 6 GDPR)

Processing shall be lawful only if and to the extent that at least one of the following applies

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary in order to protect the vital interests of the data subject or of another natural person

Lawfullness of processing (article 6 GDPR)

Processing shall be lawful only if and to the extent that at least one of the following applies

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

Other basic concepts GDPR

- risk analysis as a basis
- privacy by design
- privacy by default
- records of processing activities
- data protection impact assessment (DPIA)
- notification of personal data breach
- rights of the data subject
- data protection officer
- possibility of codes of conduct and certification
- sanctions

No “one-size-fits-all” approach

Risk-based approach: common thread

- the controller must objectively assess the likelihood and severity of the risks to the rights and freedoms of individuals when carrying out processing (common thread throughout the Regulation)

- some obligations always apply regardless of the risk; the risk can be taken into account in its implementation

- some obligations do not apply if the risk is not high

- some obligations only apply if the risk is high

Privacy by design

- the controller shall
  - take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing
  - as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing
  - implement appropriate technical and organisational measures
  - in order to meet the requirements of this Regulation and protect the rights of data subjects
- both at the time of the determination of the means for processing and at the time of the processing itself

Privacy by default

- the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed

- that obligation applies to
  - the amount of personal data collected
  - the extent of their processing
  - the period of their storage
  - their accessibility

Privacy by default: examples of measurres

- minimising the processing of personal data
- pseudonymising personal data as soon as possible
- transparency with regard to the functions and processing of personal data
- enabling the data subject to monitor the data processing
- enabling the controller to create and improve security features

Records of processing activities (article 30 GDPR)

- each controller and processor shall maintain a record of processing activities under its responsibility
- content
  - the name and contact details of the controller
  - the purposes of the processing
  - the categories of data subjects and of the categories of personal data
  - the categories of recipients of the personal data
  - the envisaged time limits for erasure of the different categories of data
  - a general description of the technical and organisational security measures
- available to the supervisory authority on request

Data Protection Impact Assessment (article 35-36 GDPR)

- where a type of processing
  - in particular using new technologies
  - and taking into account the nature, scope, context and purposes of the processing
  - is likely to result in a high risk to the rights and freedoms of natural persons
- the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (Data Protection Impact Assessment (DPIA))
- a single assessment may address a set of similar processing operations that present similar high risks

Data Protection Impact Assessment (article 35-36 GDPR)

- a DPIA is in particular required in the case of
  - a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
  - processing on a large scale of special categories of data
  - a systematic monitoring of a publicly accessible area on a large scale
- where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations

Data Protection Impact Assessment (article 35-36 GDPR)

- a Data Protection Impact Assessment is a process to help the controller identify and minimize the data protection risks
- a DPIA is completed for every processing that is likely to result in a high risk to individuals
- it is also good practice to do a DPIA for any other major project which requires the processing of personal data
- the DPIA must
  - describe the nature, scope, context and purposes of the processing
  - assess necessity and proportionality of the processing in relation to the purposes
  - identify and assess risks to the rights and freedoms of data subjects
  - identify measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR

Data Protection Impact Assessment (DPIA)

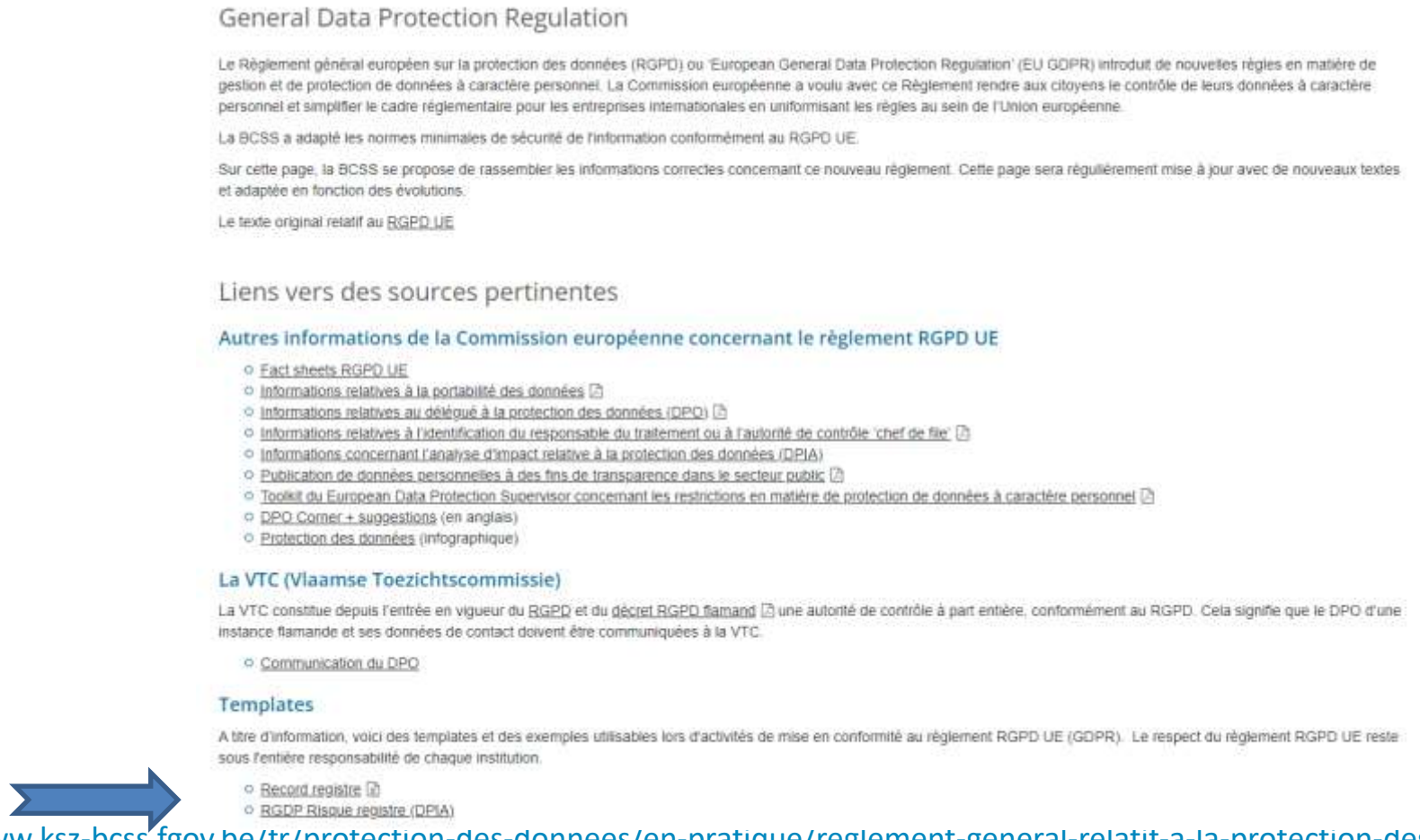
- to assess the level of risk, one must consider both the likelihood and the severity of any impact on individuals. High risk could result from
  - a high probability of some harm
  - a lower probability of serious harm

- the DPIA implicates the DPO and, where appropriate, individuals and relevant experts; any processors may also need to assist

- if a high risk is identified, the supervisory authority must be implicated before starting the processing

Executing the DPIA: example of Belgian CBSS

- CBSS has developed a template for executing the DPIA



General Data Protection Regulation

Le Règlement général européen sur la protection des données (RGPD) ou 'European General Data Protection Regulation' (EU GDPR) introduit de nouvelles règles en matière de gestion et de protection de données à caractère personnel. La Commission européenne a voulu avec ce Règlement rendre aux citoyens le contrôle de leurs données à caractère personnel et simplifier le cadre réglementaire pour les entreprises internationales en uniformisant les règles au sein de l'Union européenne.

La BCSS a adapté les normes minimales de sécurité de l'information conformément au RGPD UE.

Sur cette page, la BCSS se propose de rassembler les informations correctes concernant ce nouveau règlement. Cette page sera régulièrement mise à jour avec de nouveaux textes et adaptée en fonction des évolutions.

Le texte original relatif au RGPD UE

Liens vers des sources pertinentes

Autres informations de la Commission européenne concernant le règlement RGPD UE

- Fact sheets RGPD UE
- Informations relatives à la portabilité des données
- Informations relatives au délégué à la protection des données (DPO)
- Informations relatives à l'identification du responsable du traitement ou à l'autorité de contrôle 'chef de file'
- Informations concernant l'analyse d'impact relative à la protection des données (DPIA)
- Publication de données personnelles à des fins de transparence dans le secteur public
- Toolkit du European Data Protection Supervisor concernant les restrictions en matière de protection de données à caractère personnel
- DPO Corner + suggestions (en anglais)
- Protection des données (infographique)

La VTC (Vlaamse Toezichtscommissie)

La VTC constitue depuis l'entrée en vigueur du RGPD et du décret RGPD flamand une autorité de contrôle à part entière, conformément au RGPD. Cela signifie que le DPO d'une instance flamande et ses données de contact doivent être communiquées à la VTC.

- Communication du DPO

Templates

A titre d'information, voici des templates et des exemples utilisables lors d'activités de mise en conformité au règlement RGPD UE (GDPR). Le respect du règlement RGPD UE reste sous l'entière responsabilité de chaque institution.

- Record registre
- RGDP Risque registre (DPIA)

https://www.ksz-bcss.fgov.be/fr/protection-des-donnees/en-pratique/reglement-general-relatif-a-la-protection-des-donnees

First sheet: basic screening

- basic screening determines whether a DPIA is required

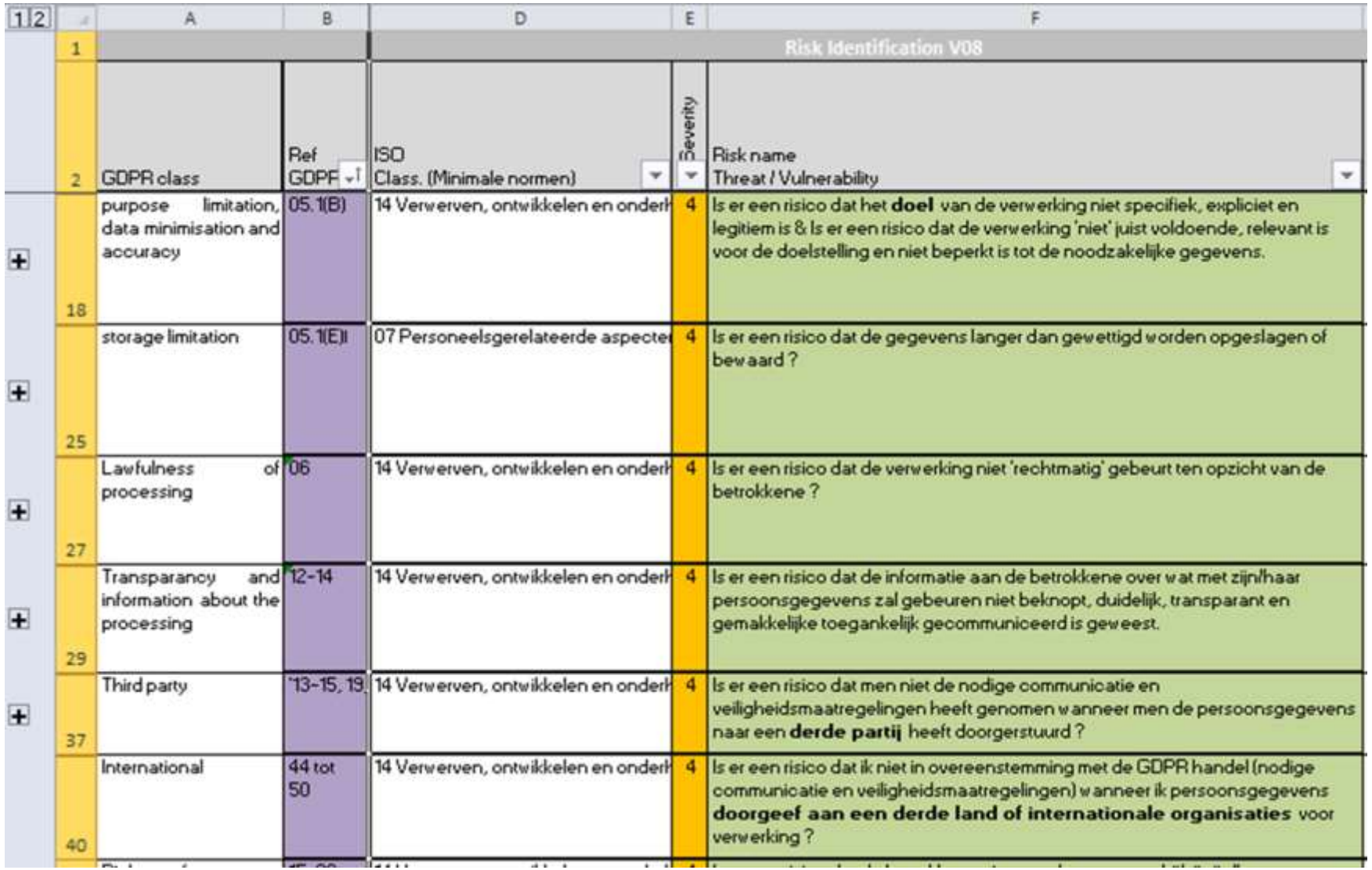
- developed based on following criteria
  - article 35 GDPR
  - consideration 75 GDPR
  - recommendation of the Belgian Data Protection Authority
  - Working Party 29 – guidelines for DPIA

- as soon as 2 risks are present, the DPIA is required

Second sheet: risk assessment & management

- if a DPIA is required, perform a risk assessment of the processing
  - check what risks in the tool are relevant for the processing
  - the controller participates in this part of the exercise
- next, describe the existing information security and data protection measures in the DPIA
- consider the residual risks
- if the residual risks are above the acceptable level, try to apply additional information security and data protection measures in order to get the residual risk under the acceptable level of risk
- in case residual risks above acceptable level cannot be remediated, the controller has to consult the Data Protection Authority before starting the processing

Template: list of risks based on GDPR



	A	B	D	E	F
1			Risk Identification V08		
2	GDPR class	Ref GDPR	ISO Class. (Minimale normen)	Severity	Risk name Threat / Vulnerability
18	purpose limitation, data minimisation and accuracy	05. 1(B)	14 Verwerven, ontwikkelen en onderh	4	Is er een risico dat het **doel** van de verwerking niet specifiek, expliciet en legitiem is & Is er een risico dat de verwerking 'niet' juist voldoende, relevant is voor de doelstelling en niet beperkt is tot de noodzakelijke gegevens.
25	storage limitation	05. 1(E)I	07 Personeelsgerelateerde aspecte	4	Is er een risico dat de gegevens langer dan gewettigd worden opgeslagen of bewaard ?
27	Lawfulness of processing	06	14 Verwerven, ontwikkelen en onderh	4	Is er een risico dat de verwerking niet 'rechtmatig' gebeurt ten opzicht van de betrokkene ?
29	Transparancy and information about the processing	12-14	14 Verwerven, ontwikkelen en onderh	4	Is er een risico dat de informatie aan de betrokkene over wat met zijn/haar persoonsgegevens zal gebeuren niet beknopt, duidelijk, transparant en gemakkelijke toegankelijk gecommuniceerd is geweest.
37	Third party	'13-15, 19,	14 Verwerven, ontwikkelen en onderh	4	Is er een risico dat men niet de nodige communicatie en veiligheidsmaatregelingen heeft genomen wanneer men de persoonsgegevens naar een **derde partij** heeft doorgerstuurd ?
40	International	44 tot 50	14 Verwerven, ontwikkelen en onderh	4	Is er een risico dat ik niet in overeenstemming met de GDPR handel (nodige communicatie en veiligheidsmaatregelingen) wanneer ik persoonsgegevens **doorgeef aan een derde land of internationale organisaties** voor verwerking ?

Template: risk evaluation

Initial risks and risk mitigation (security controls) → Remaining risks

Ref GDP	Severity	Risk name Threat / Vulnerability	Risk description Impact / Probability / Costs	Prob. (1-5)	Imp. (1-5)	Current controls descriptio	Cont. (1-5)	Residual	Tolerate	Treat	Transfer	Terminate	Plans proposal Mitigation / Contingency
05.1(B)	4	Is er een risico dat het **doel** van de verwerking niet specifiek, expliciet en legitiem is & Is er een risico dat de verwerking 'niet' juist voldoende, relevant is voor de doelstelling en niet beperkt is tot de noodzakelijke gegevens.		4	4		3	1					
05.1(E)I	4	Is er een risico dat de gegevens langer dan gewettigd worden opgeslagen of bewaard ?		4	4		3	1					
06	4	Is er een risico dat de verwerking niet 'rechtmatig' gebeurt ten opzicht van de betrokkene ?		4	4		3	1					

PROBABILITY Level				
RARE	OCCASIONAL	POSSIBLE	REGULAR	OFTEN
1	2	3	4	5
p < 10%	21% < p < 50%	31% < p < 70%	71% < p < 90%	p > 90%
The event occurs only in very exceptional circumstances	The event only occurs in certain circumstances	The event could occur at some point	The event should occur at some point	The event is likely to occur in most circumstances

	IMPACT Level				
	VERY LOW	LOW	MEDIUM	HIGH	CRITICAL
	1	2	3	4	5
Costs	Exceeding < 1%	Exceeding < 5 %	Exceeding < 10 %	Exceeding < 20 %	Exceeding > 20 %
Quality	Non-compliance with negligeable requirements	Non-compliance with requirements for minors isolated cases	Non-compliance with requirements and in some cases, which would require the establishment of 'work-around'	Non-compliance with important requirements, which would lead to concessions for the project	Non-compliance with basic requirements, which can put the project in jeopardy
rights and freedom of natural person (*)	rights and freedom are never impacted	rights and freedom are occasionally impacted	rights and freedom are regularly impacted	rights and freedom are often impacted	rights and freedom are always impacted
Schedule	Negligeable delay	Project delay < 5%	Project delay < 10%	Project delay < 20%	Project delay > 20%

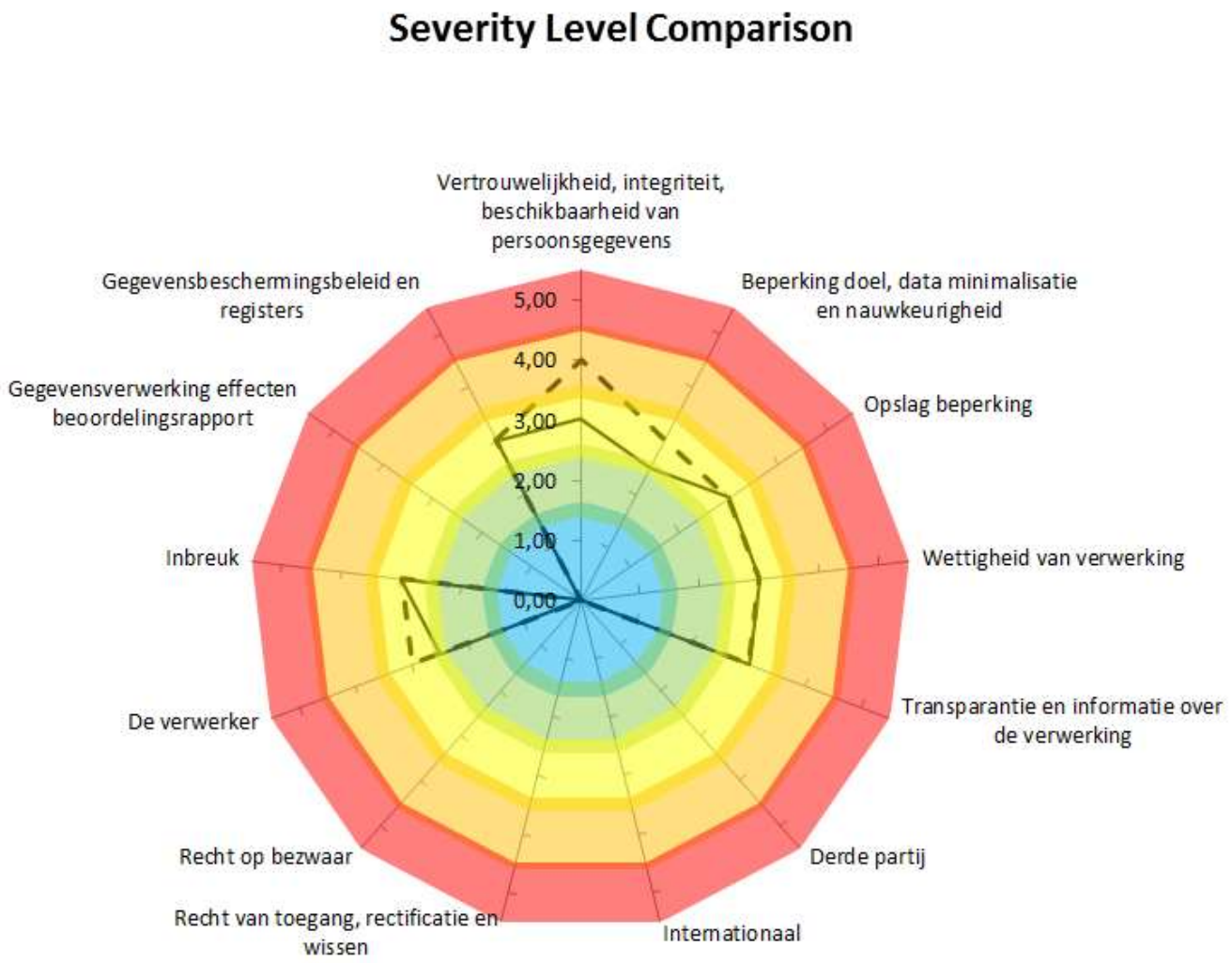
	CURRENT CONTROL Level				
	VERY WEAK	WEAK	MEDIUM	HIGH	VERY HIGH
	1	2	3	4	5
Maturity Level : summary	Initial / Ad hoc	Non formel / Répétitif	Systématique / Défini	Intégré / Mesuré	Optimisé
Maturity Level : description	Conscience du risque & Conscience de contrôle interne	Contrôle interne sans procédures et pas connu par tous les employés de SMALS	Procédures exhaustives & Formations sur le contrôle interne	Améliorations continues & Révisions du contrôle interne	Contrôle en temps réel

Template: heat maps initial risk

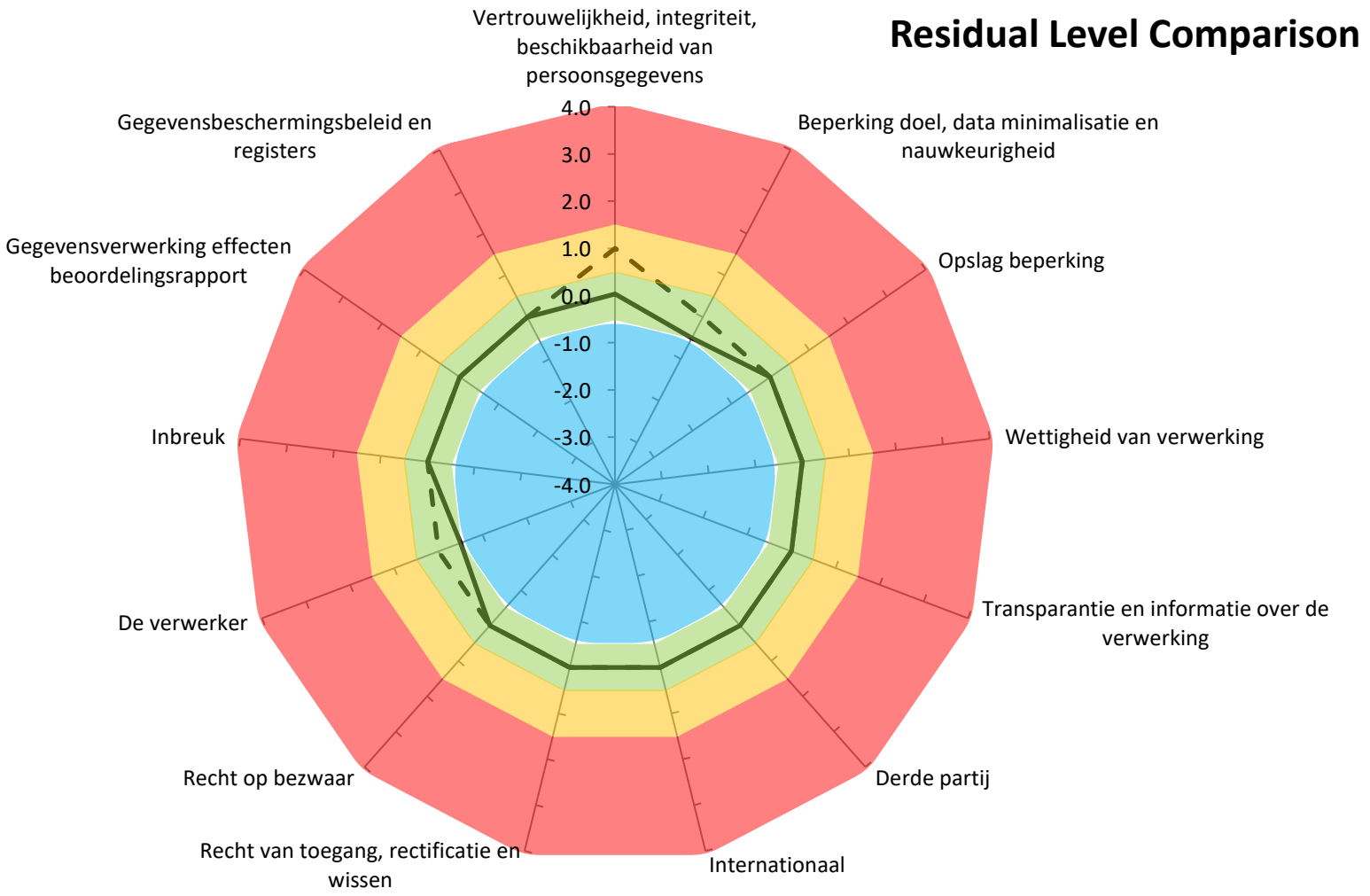
Risk Map	Prob.					
Imp.	1	2	3	4	5	Grand Total
5	1	1		1		3
4	1	5	7	4	1	18
3		2	7	2		11
2		1	3	5		9
1						
Grand Total	2	9	17	12	1	**41**

Summary	
Negligeable Risks	0
Acceptable Risks	7
Moderate Risks	**28**
Important Risks	**6**
Critical Risks	**0**

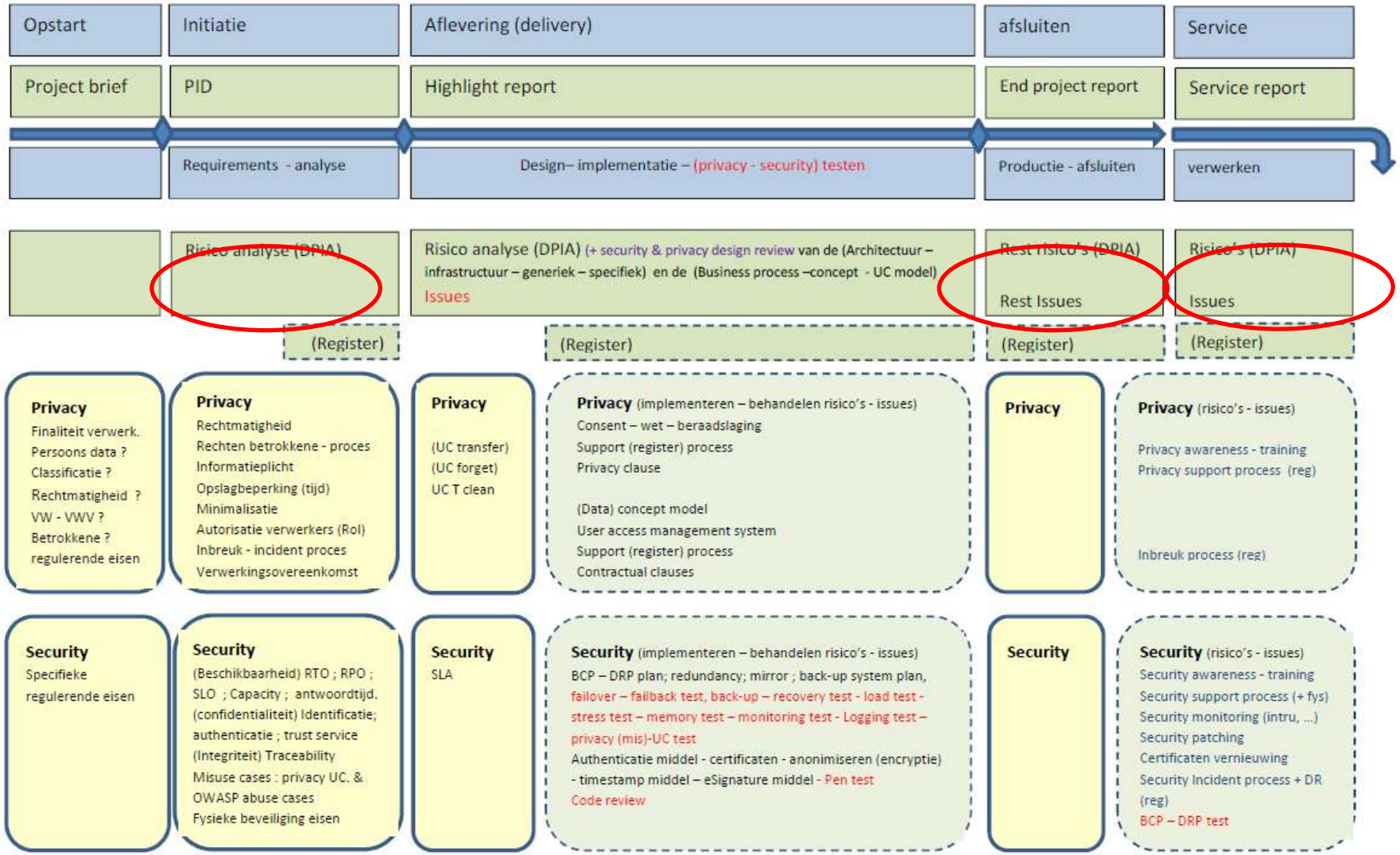
Template: intermediate result



Template: end result



DPIA: as from start up of project to delivery



DPIA and production services

- during the lifecycle of a service, it is advised to regularly review the DPIA
  - changing conditions
  - major changes to technology
  - changing risks on the market

- CBSS do review the DPIAs every 3 years

Notification of personal data breach (article 33-34 GDPR)

- in case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

- when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay

Notification of personal data breach (article 33-34 GDPR)

- the communication to the data subject is not required if
  - the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption, or
  - the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize, or
  - it would involve disproportionate effort; in such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner

Rights of the data subject (article 12-22 GDPR)

- right to be informed
- right of access
- right to rectification
- right to erasure (right to be forgotten)
- right to restriction of processing
- notification obligation regarding rectification or erasure of personal data or restriction of processing
- right to data portability
- right to object
- right not to be subject to a decision based solely on automated processing, including profiling

Data Protection Officer (DPO) (article 37-39 GDPR)

- mandatory if
  - controller is a public authority
  - controller's core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
  - controller's core activities consist of processing on a large scale of special categories of data
- optional in other situations
- independency, no conflict of interests
- expert knowledge of information security and data protection

Data Protection Officer (DPO) (article 37-39 GDPR)

- tasks of the Data Protection Officer (DPO)
  - to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR
  - to monitor compliance with GDPR and with the policies of the controller or processor in relation to the protection of personal data, including
    - the assignment of responsibilities
    - awareness-raising and training of staff involved in processing operations
    - related audits
  - to provide advice where requested as regards the DPIA and monitor its performance
  - to cooperate with the supervisory authority and to act as the contact point for the supervisory authority on issues relating to processing

Data Protection Officer (DPO) (article 37-39 GDPR)

- controller ensures that
  - the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data
  - the DPO does not receive any instructions regarding the exercise of those tasks
  - is not dismissed or penalised by the controller or the processor for performing his tasks
- controller supports the DPO in performing its tasks
  - by providing resources necessary to carry out those tasks
  - by providing access to personal data and processing operations
  - by maintaining his or her expert knowledge
- the DPO directly reports to the highest management level of the controller or the processor
- the DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks

Minimal information security standards

- developed by information security working party composed of Data Protection Officers (DPOs) of the actors => buy in !
- approved by an independent Information Security Committee designated by Parliament
- based on ISO 27000 standards, adapted for social security and health care (see https://en.wikipedia.org/wiki/ISO/IEC_27000-series)
- defines 15 areas of security
- enforced for all actors in the social sector
- extended with policy guidelines
  - minimal standards refer to policy guidelines for more detail
  - policy guidelines provide support for concrete implementation

Topics covered by minimal information security standards

- basic principles
- information security policies
- organisation of information security
  - internal organisation
  - mobile equipment and remote working
- security measures for employees and co-workers
- management of company assets
- physical and environmental security
- access control (physical and logical)
- encryption

Topics covered by minimal information security standards

- operations management
- protecting communications
- procurement, design, development and maintenance of systems
- supplier management
- incident management
- business continuity
- compliance

Minimal standards: data classification

- 5 levels of data sensitivity classification
  - 4 -> top secret
  - 3 -> secret, high classified
  - 2 -> confidential, classified
  - 1 -> unclassified, sensitive
  - 0 -> unclassified, public
- each type of data is linked to a sensitivity classification
  - see next slide
- each type of classification has the data handling guidelines
  - how to transport,
  - use in test, development, acceptance,
  - authentication level for access,
  - ….

Minimal standards: data classification

Aperçu type de donnée et classe de sensibilité par défaut

Type de données (informations) groupes	Classe de sensibilité
1. DONNEES PUBLIQUES **I. Données publiques**	non classée
2. DONNEES INTERNES **II. Données internes**	limitée
3. DONNEES D'ENTREPRISE CONFIDENTIELLES **III. Données d'entreprise confidentielles**	confidentielle
4. DONNEES A CARACTERE PERSONNEL **IV. Données à caractère personnel**	confidentielle
5. DONNEES SOCIALES A CARACTERE PERSONNEL **V. Données sociales à caractère personnel)**	confidentielle
6. DONNEES SENSIBLES A CARACTERE PERSONNEL **VI. Données médicales à caractère personnel** **X Catégories spécifiques de données à caractère personnel** **XI Données à caractère personnel relatives aux condamnations pénales et aux infractions**	très confidentielle
7. DONNEES MEDICALES A CARACTERE ADMINISTRATIF **VII Données médicales à caractère administratif**	confidentielle
8. DONNEES CLASSIFIEES (loi du 11/12/1998) **VIII Données classifiées (loi du 11/12/1998)**	très secrète, secrète, confidentielle
9. DONNEES PRIVEES **IX Données privées**	confidentielle
10. DONNEES D'ENTREPRISE TRES CONFIDENTIELLES **XII. Données très confidentielles de l'entreprise**	très confidentielle

Structural and institutional measures

- no unnecessary central data storage
- availability of free of charge, basic information security services
  - user- & access management
  - encryption
  - logging
  - reference directories
  - …
- independent Information Security Committee designated by the Parliament that authorizes data exchange
- a preventive control of the legitimacy of personal data exchange by an trusted third party (TTP) according to the authorizations of the independent Information Security Committee

Considerations in the deliberations

- lawfulness and purpose limitation
  - is the processing serving a legitimate purpose?
  - are the purposes of the processing well defined ?
- data minimization
  - is the processing using the minimal dataset to achieve the purposes ?
  - storage limitation
- integrity and confidentiality
  - measures on how to guarantee both parameters
- transparency for the data subjects
- information security standards

Organisational measures

- information security department headed by Data Protection Officer (DPO) with each actor in the social sector
- specialized information security service providers
- need for compliance with minimal information security and data protection standards (Minimale normen / Normes minimales)
- information security working parties developing information security policies
- Data Protection Impact Assessments (DPIA)
- unique file

Organisational measures

- yearly assessment of compliance with minimal security standards
  - questionnaire sent out to all institutions connected to the network
  - checked by the security service of the TTP
  - reviewed in the Information Security work group
- security requirements reviewed on regular basis
- internal audits with continuous improvement plans => independent auditor reporting on findings

Information Security Department

- legal obligation
  - assignment of a DPO
  - advices controller on privacy and security
  - can be assigned additional tasks as long as this does not conflict with the mission of a DPO
- role of the information security department
  - each institution has to set up a security department
    - stimulates information security (minimal security standards, awareness creation, education, …)
    - documents the information security related topics (DPIA, registers)
    - advises and checks on compliance (internal audits)
    - reports on information security and privacy
  - the DPO the is head of the security department

Unique file

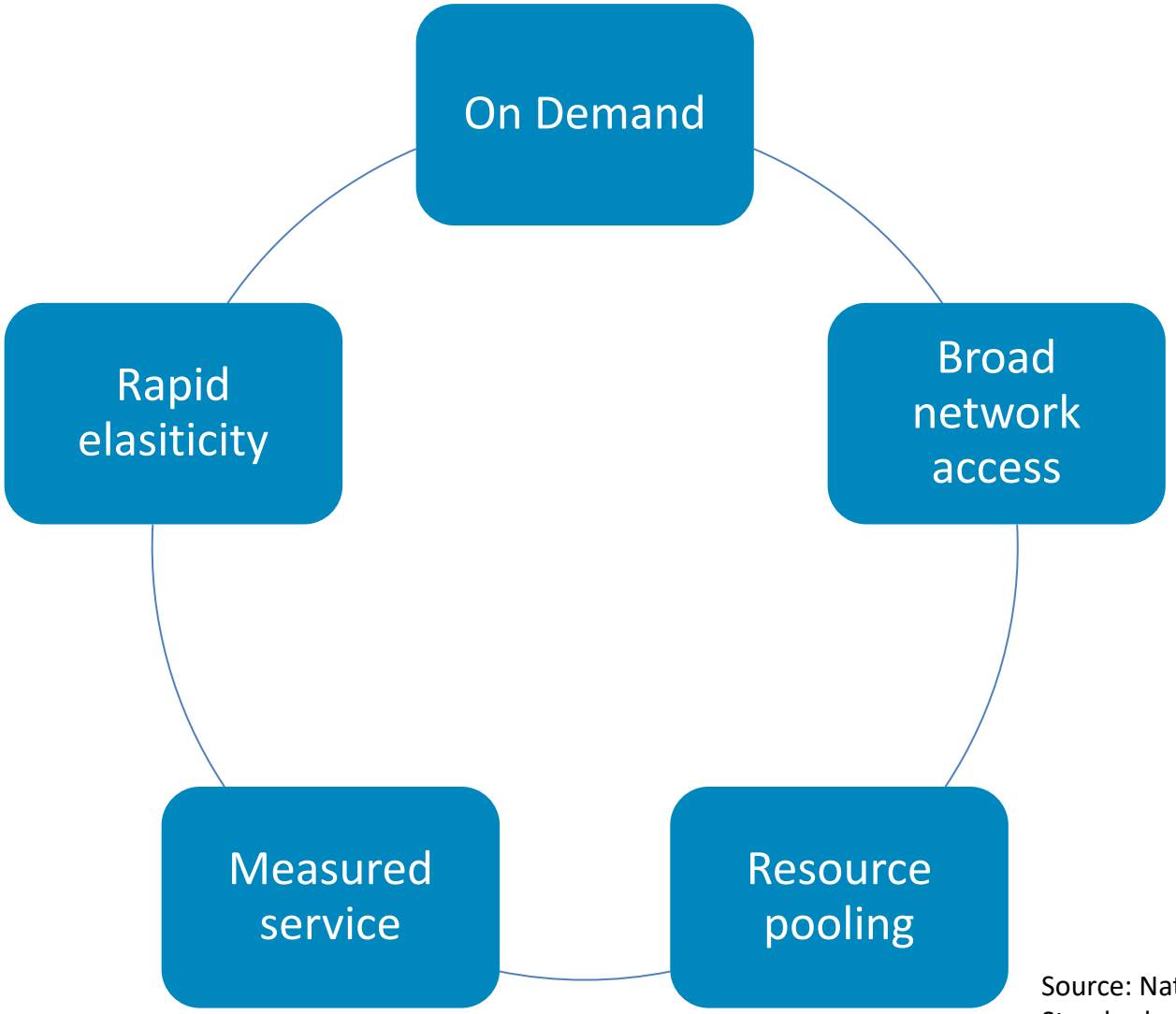
- goals
  - centralizing all information required to approve the service prior to commissioning the service in line with guidelines regarding information security and data protection
  - meeting the documentation requirement of GDPR
- content
  - purposes of the processing
  - high level technical design
  - categories of data subjects and data
  - types of users
  - security measures, ao
    - user authentication level
    - user authorization system
    - user activity logging
  - DPIA if available
- elaborated for every new service
- updated and approved for major changes to existing services

Circles of trust

- agreements between actors about
  - who is responsible of carrying out which authentications and verifications on the basis of which means
  - how the results of the authentications and verifications are securely stored and exchanged electronically between the actors involved
  - who is responsible of logging access (attempts) to the services and applications
  - how it is ensured that a complete reconstruction of loggings can take place to determine which natural person has used which service in relation to which person, when and for what purposes
  - the retention period of the loggings, as well as the way in which these can be consulted by those who are entitled to do so

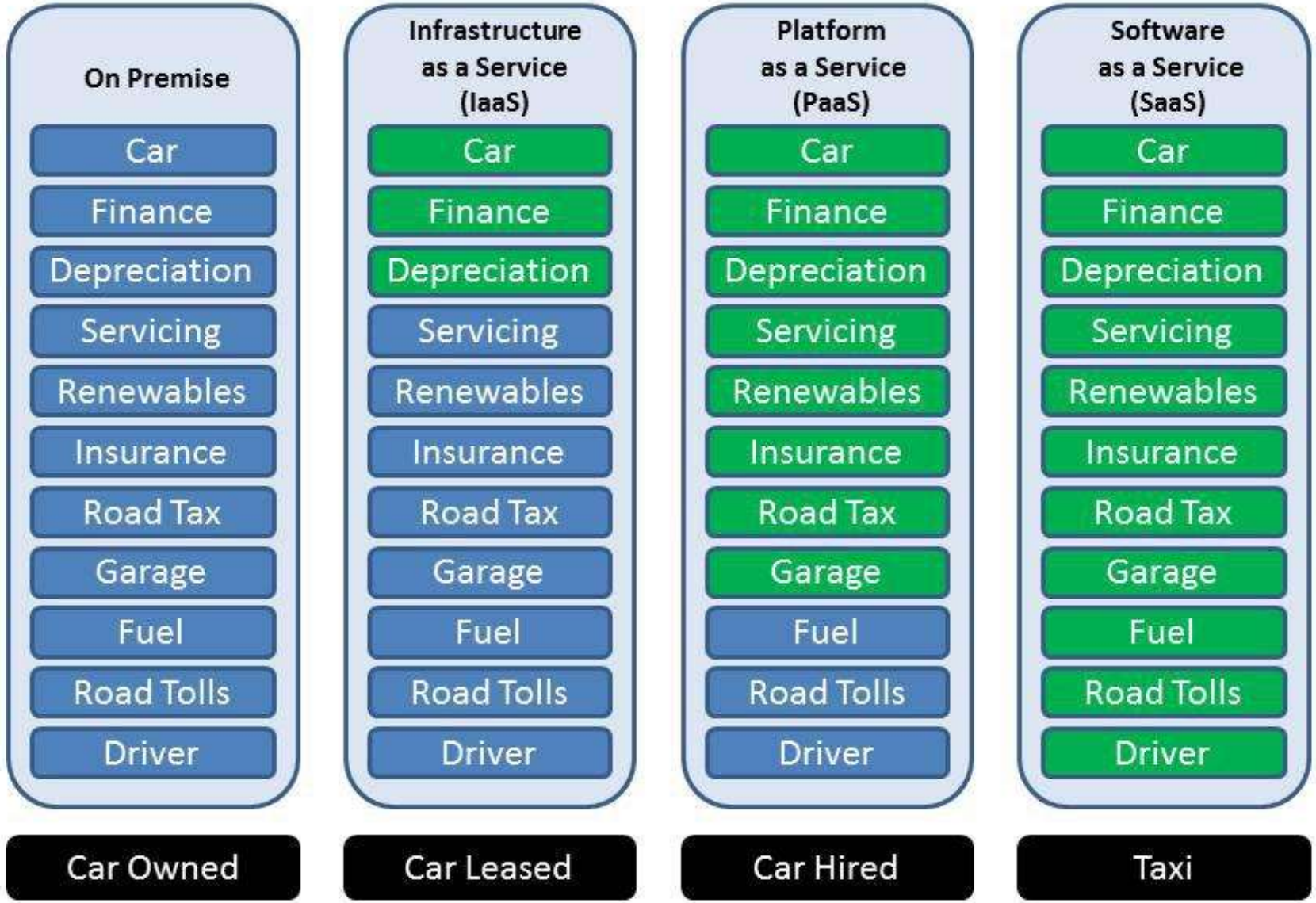
G-Cloud

What is “cloud” ?



Source: National Institute for Standards and Technology, USA

Car as a Service(CaaS)



As a service : major characteristics

- self service: industrialised & automated
- available: immediate availability
- extensible/elastic: scale up or down
- shared: multiple users for scale effects
- use based invoicing: based on real use of resources
- low entry barrier: complexity is hidden for user
- incremental service changes

Cloud service models

IaaS

- Infrastructure as a Service
- basic IT infrastructure components (e.g. Amazon virtual machines)

PaaS

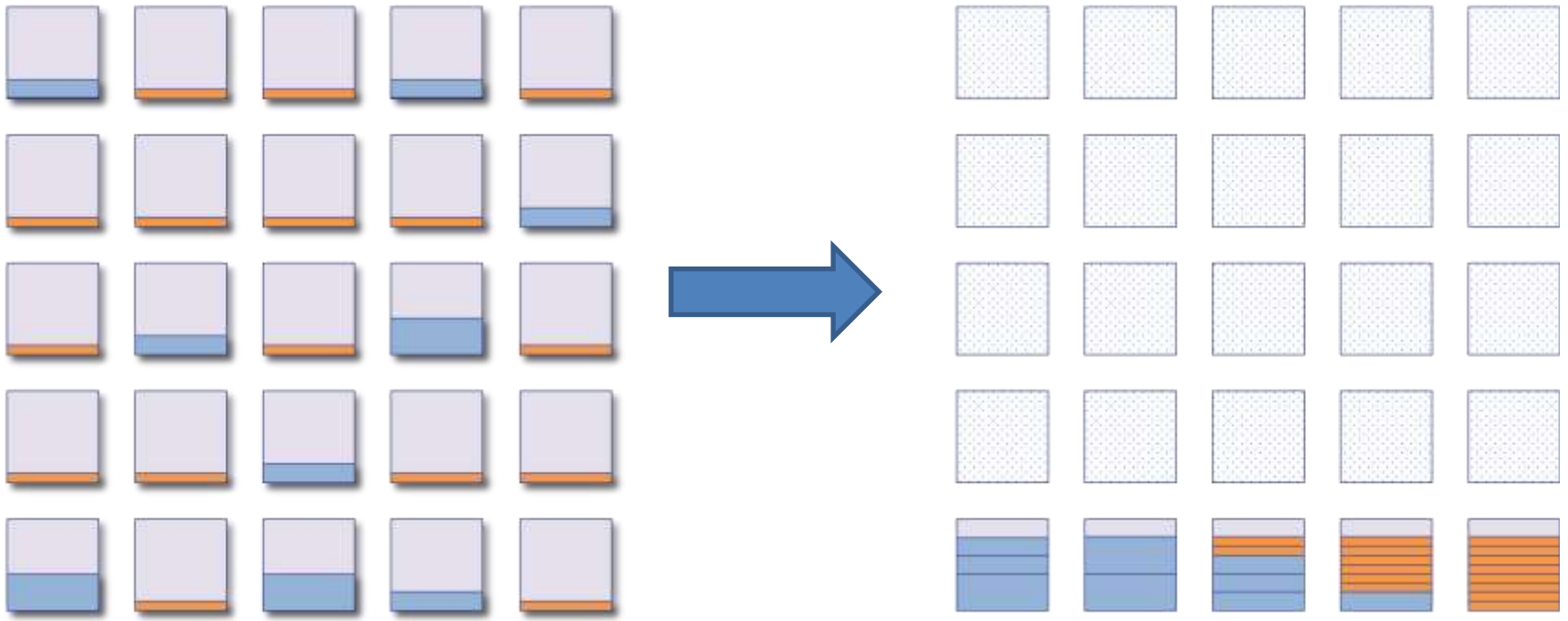
- Platform as a Service
- platforms to build applications

SaaS

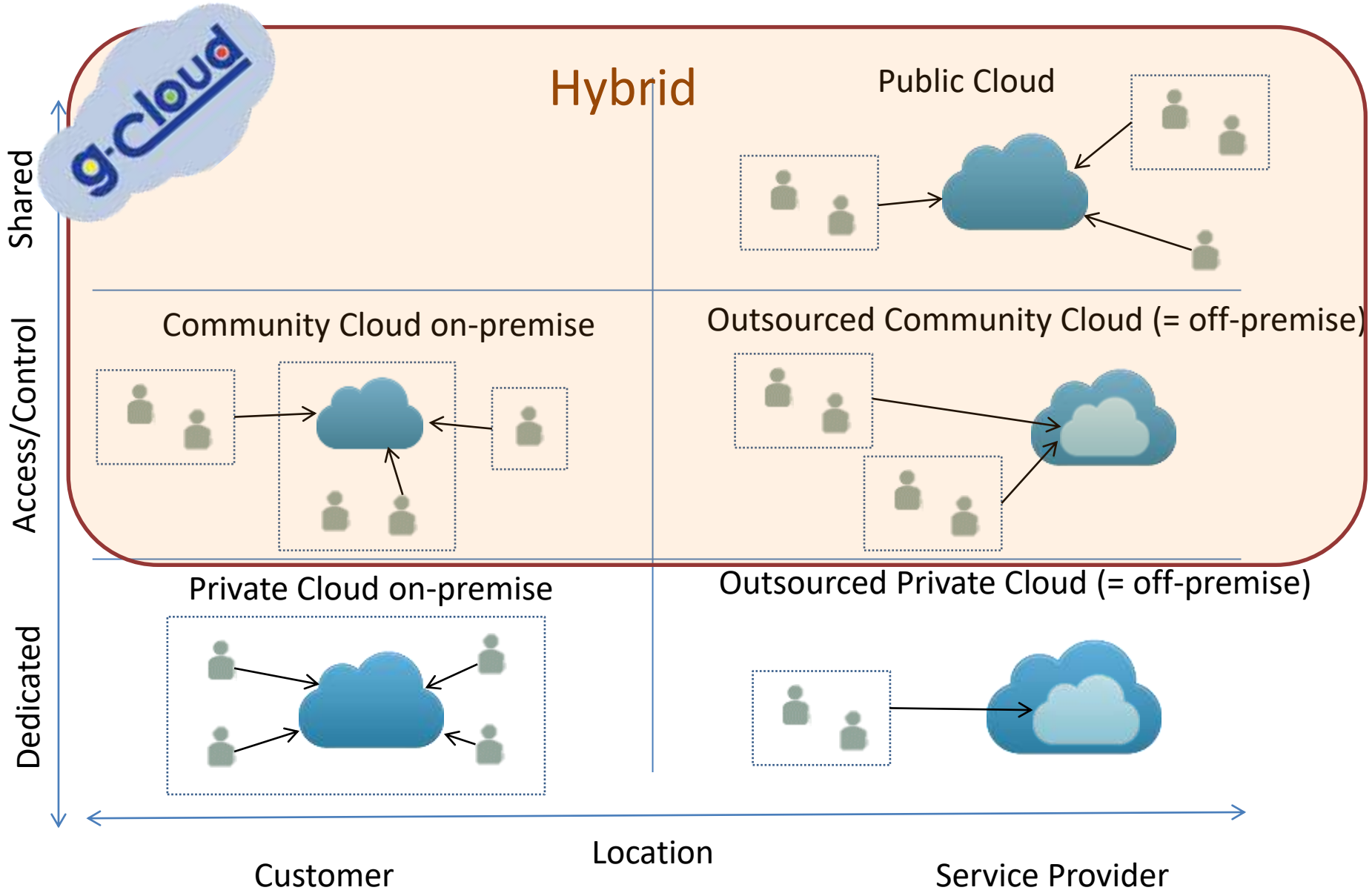
- Software as a Service
- full applications (e.g. O365, Google Apps, …)

Virtualisation

- consolidation of physical resources
- > 70% “easy consolidation”
- first step to cloud (“dematerialisation”)



Cloud deployment types



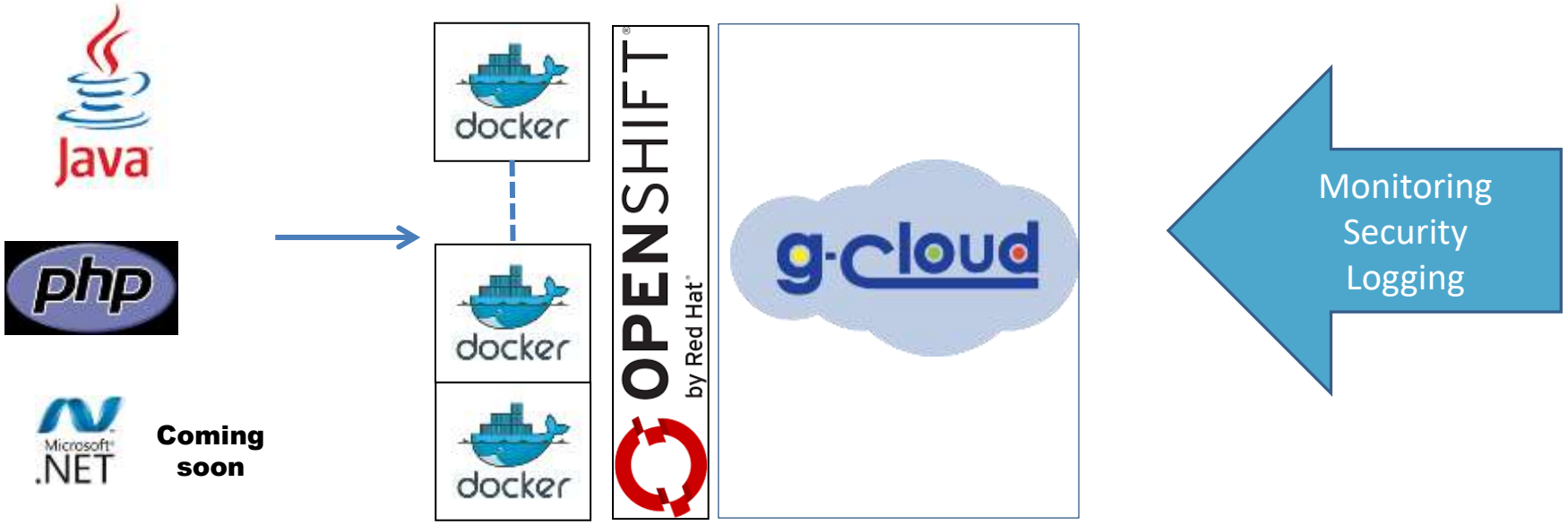
Cloud advantages

- any place, any time, anywhere : mobile
- safeguarded with backups
- high level of security if well implemented
- lower Total Cost of Ownership (TCO)
- stability & incremental updates
- collaboration
- should provide portability
- community cloud solutions
  - can be open for integration with other services
  - trust relationship / data protection (e.g. Vitalink)

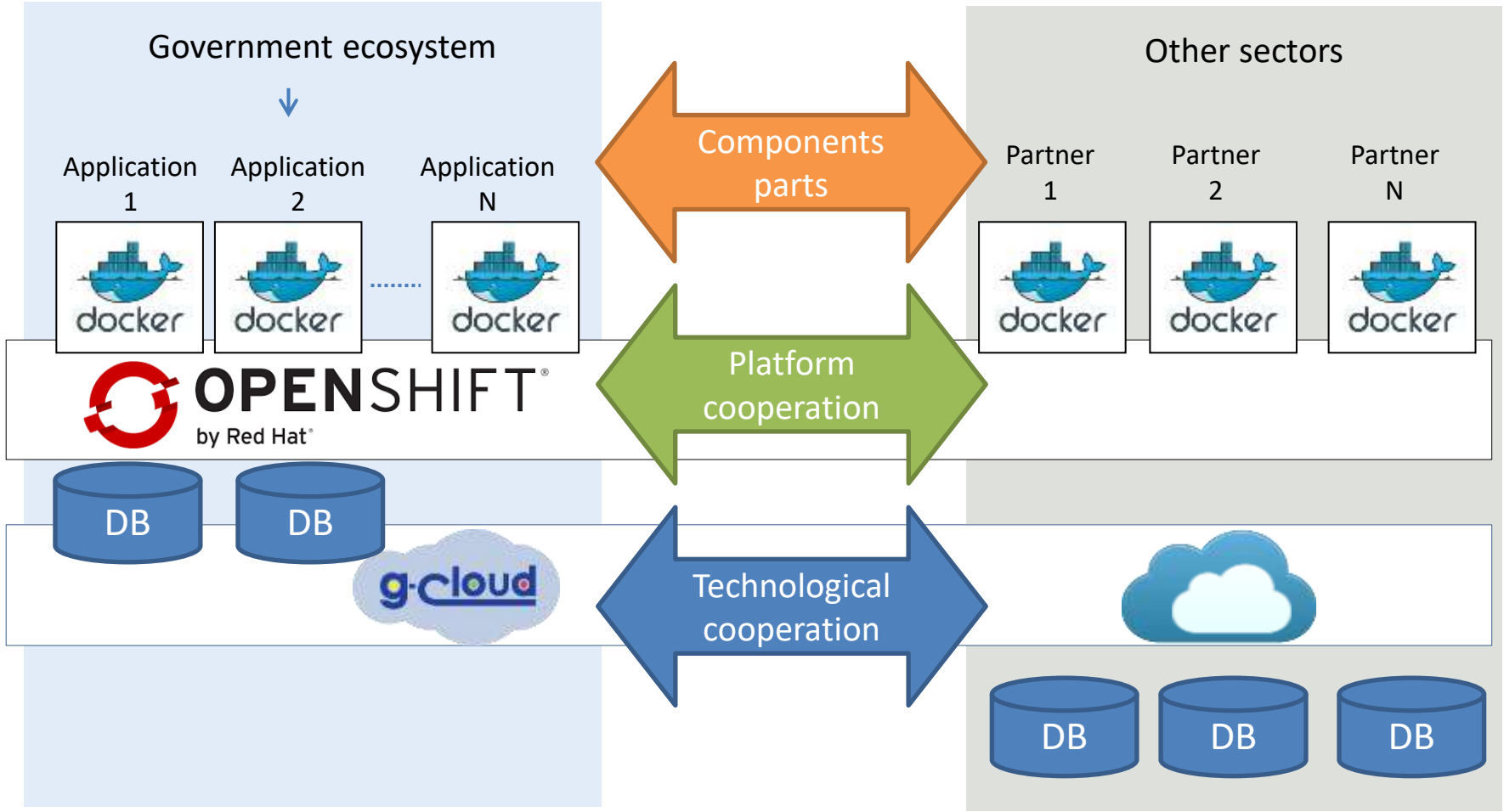
PaaS in (G-)cloud - containers

- introducing container technology

- translated into modern technology such as Platform-as-a-Service



New ways of cooperation



Public cloud - main issues

- longitudinal confidentiality of personal data
  - need for comprehensive longitudinal encryption of personal data
  - in motion, at rest and in use
- performant continuous availability of applications and data
- easy migration of applications and data
- compliance with GDPR / Schrems II

Intermediate solution

- need for overall government positioning
  - eGov public cloud policy
  - based on information classification
  - appropriate organizational, technical & contractual measures
  - hybrid approach
    - pure public cloud not suited for sensitive use cases
    - secure private cloud on-premise for secret and top secret
    - hybride (community on-premise and public) cloud for other levels

Belgian example

What is G-Cloud ?

A program including synergy projects

Synergy for existing as well as new services

For public services

Managed by public services

In cooperation with the **private sector**

What is G-Cloud ?

- shared public ICT platform
  - current target: federal state (FPS, PPS, public institutions of social security, institutions of public benefit)
  - can be extended to other interested authorities
- hybrid community cloud model
  - use of public cloud if possible
  - private community cloud hosted in data centers, managed by the government
  - operational implementation with strong involvement of the private sector

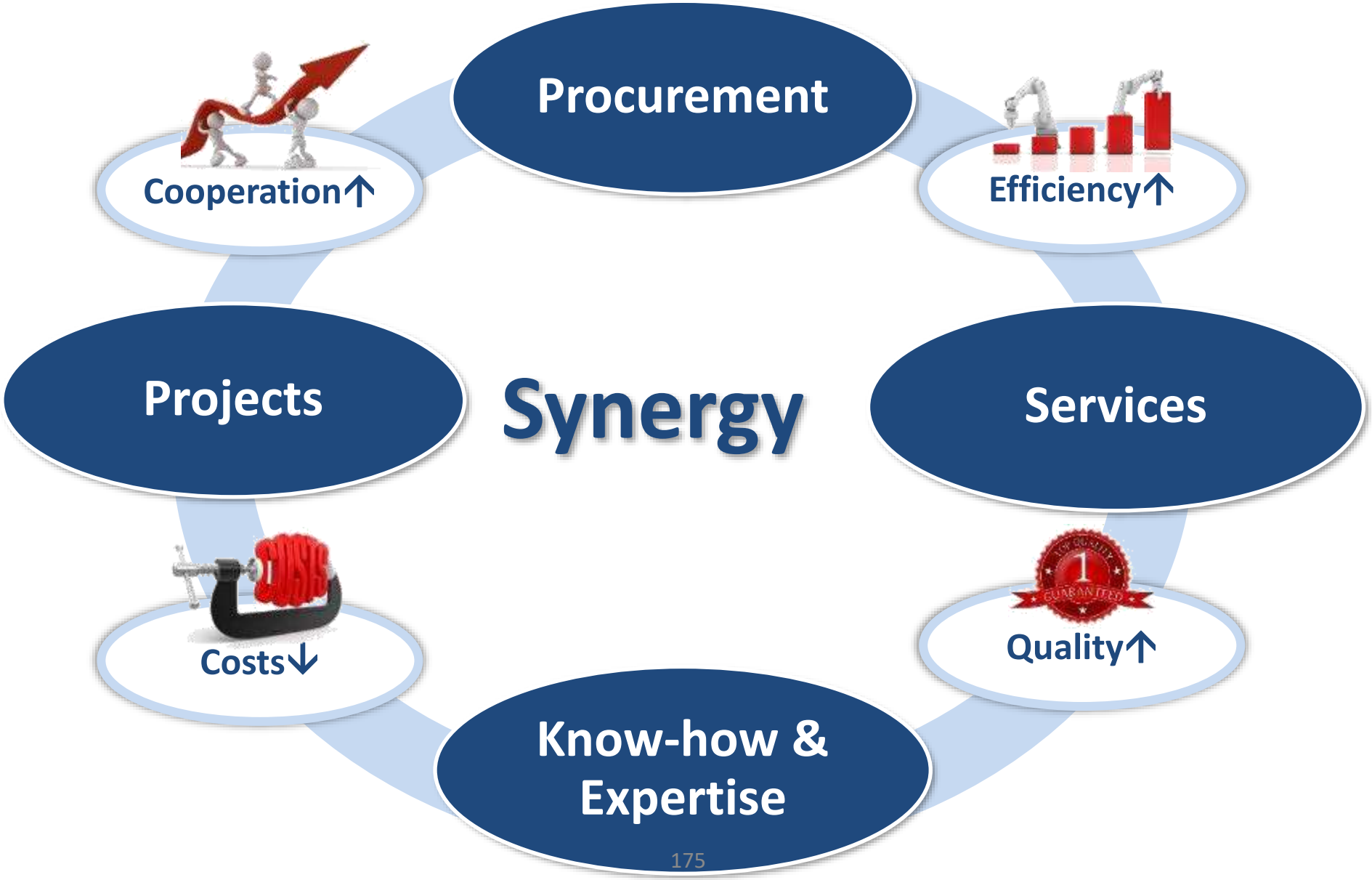
Basic principles

- maximum synergy when possible and when generating efficiency gains and/or savings while maintaining or improving the quality of the services provided to the customer

- in line with the synergy program: assignment to the one who is the most capable of proposing a form of shared services

- synergy based on result orientation, sense of responsibility and trust

G-Cloud ‘products’



Why G-Cloud?

Creation of **economies of scale**: efficiency and high quality/availability

Respect of **confidentiality** and **data protection**

Bigger **focus on business applications and flexibility** in order to realize them

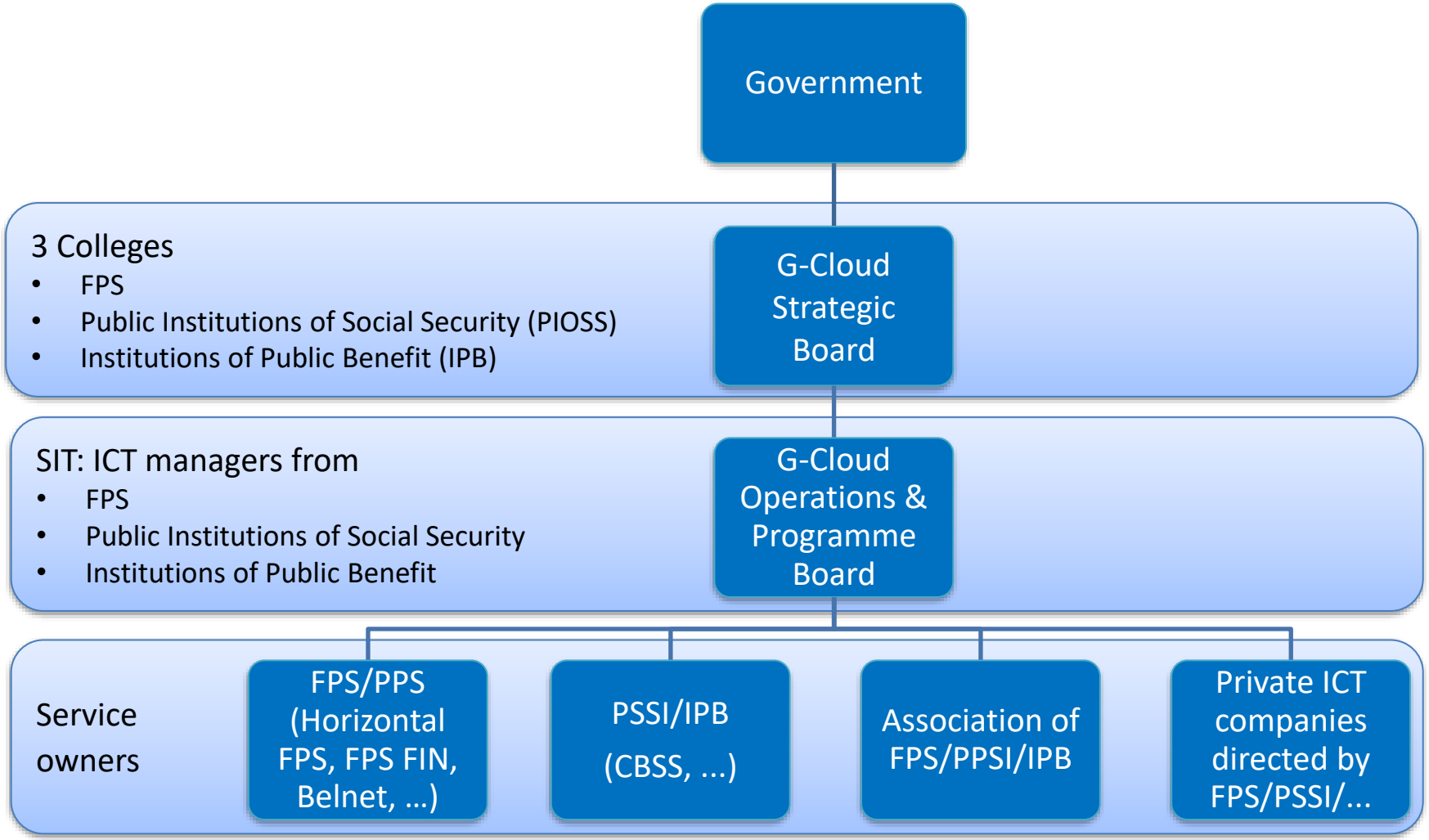
Why G-Cloud?

Greater weight during negotiations with suppliers

Pooling of knowledge and resources

Technological evolution faster available for everyone

G-Cloud organization



G-Cloud organization

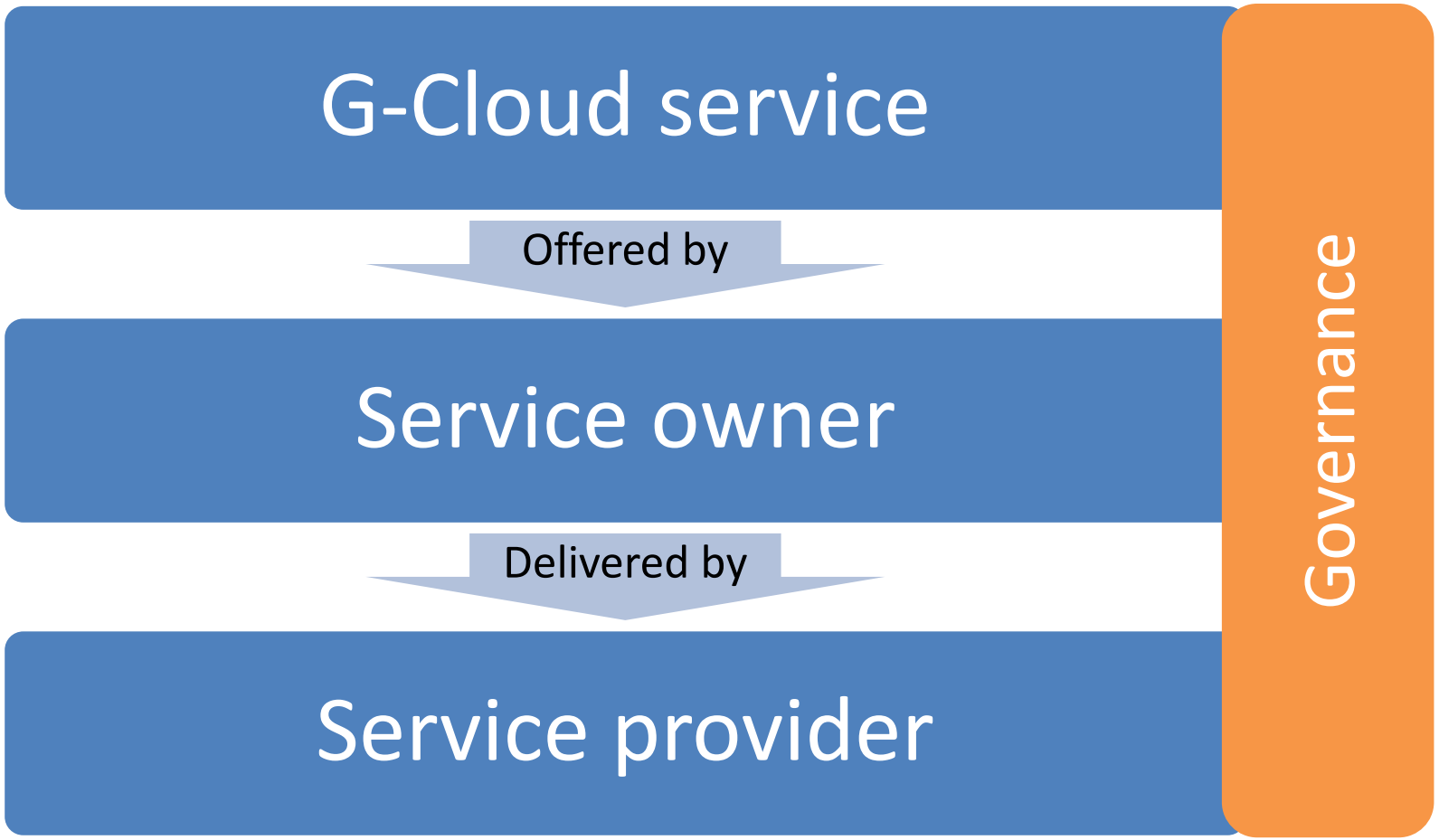
G-Cloud Strategic Board: strategic direction by senior officials

G-Cloud Operations & Program Board:

CIOs for operational direction

G-Cloud service model

- G-Cloud = coalition
- G-Cloud ≠ central organization



G-Cloud service model

- Service Owner
  - organization responsible for the service
  - develops the service and its further evolution
  - provides SLA, financial model, support model...
  - “contract” with clients
- Service Provider
  - “contract” with Service Owner
  - provides the service as agreed upon in the specifications/SLA
- Sometimes: Service Owner = Service Provider

G-Cloud P&O

- 3500 IT professionals in the federal government
- war for talent & reversed age pyramid
- cooperation model across institutional boundaries

Opportunities and challenges

Opportunities

- Flexibility
- Quality
- Economies of scale
- Self-service
- Cooperation
- Cost management

Challenges

- Security
- Confidentiality
- Continuity
- Know-how
- Strategic management

G-Cloud success factors

- efficiency
- adequate security measures (risk↘)
- optimal cooperation and trust between the institutions
- differentiation of the offer: neither ‘one size fits all’ nor tailor-made work
- capacity management
- a phased approach, no ‘big bang’
- quality of service: respect of SLAs

G-Cloud portfolio (www.gcloud.belgium.be)

SOFTWARE - STANDARD COMPONENTS AND APPLICATIONS

- **BABELFED**
- **UCC** SHAREPOINT BASIC O365
- **REGISTER**
- **IT SERVICE MANAGEMENT**
- **BECONNECTED**
- **GOVSHARE** SHAREPOINT PLATFORM
- **CSAM** AANMELDEN, BTB, SSM
- **IWF** INTELLIGENT WEB FORMS
- **WEB CONTENT MANAGEMENT**

PLATFORM - DEVELOPMENT AND SPECIALIZED TECHNICAL TOOLS

- **GREENSHIFT** OPEN SOURCE PAAS
- **YELLOWSHIFT** MICROSOFT PAAS
- **BLUE STACK DB** IBM DB
- **SERVICE PLATFORM**

INFRASTRUCTURE - SERVICES ("SOFT" INFRA)

- **UCC** VOICE/IM
- **UCC** EXCHANGE ON PREMISE
- **SHAD** SHARED DIRECTORY
- **ARCHIVING**
- **UCC** CONTACT CENTER
- **UCC** EXCHANGE O365
- **INTERNET ACCESS PROTECTION SECURITY AS A SERVICE**
- **BACKUP**
- **UCC** MOBILE DEVICE MANAGEMENT

INFRASTRUCTURE- FOUNDATION ("HARD" INFRA)

- **COMPUTE** VIRTUAL MACHINE
- **HOUSING**
- **FEDWAN**
- **STORAGE**
- **COMPUTE** HYPERVISOR
- **FEDMAN**

Data classification

- information classification model drafted within « Federal Information Security Policy » (FISP)
  - https://dt.bosa.be/nl/federaal beleid_voor_informatiebeveiliging_fisp
- definition of levels

- classification based on the impact of the loss or dissemination of information
  - impact for government (agencies)
  - impact on privacy rights
- practical classification explained in privacy vademecum
  - https://dt.bosa.be/sites/default/files/fisp_-_privacy_vademecum_nl.pdf

G-Cloud impact - shared procurement

- cooperation regarding the public procurements
  - juridical: central procurement agency clause
  - know-how: specialized in ICT purchases
  - simplicity: less administrative work for the private sector and the state
  - possibility to accelerate the purchases and to avoid double specifications procedures
  - price reductions thanks to the volume
- software licences
  - negotiations with the providers
  - mutual exchange of unused licences

Thank you

Make sure to answer our survey that will appear on your browser, and join us for the next sessions!

+ know more and become a member of

socialprotection.org