WORLD BANK GROUP

ID4D
IDENTIFICATION FOR DEVELOPMENT

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

The Dutch Government´s Strategy for Digital Identity

Building trust in the digital world

Michiel van der Veen

Director for Innovation & Development at *the National Office for Identity Data*

Wouter Welling

Coordinating Policy Officer Digital Identity at *Ministry of the Interior and Kingdom Relations*

The World Bank Group's ID4D Initiative is hosting a series of interactive webinars on ID ecosystems from around the world. The first webinar in this series is on the Dutch government's strategy for digital identity. Michiel van der Veen and Wouter Welling will present the government's strategy.

The presentation will cover the government's plans for:

- Reliable data-sharing, organizing access to digital services;

- Issuing a recognized foundational digital identity;

- Establishing the accompanying laws and regulations; and

- Enabling people to interact with business across the EU under eIDAS regulation.

Agenda

1) The Dutch identity ecosystem

2) Dutch strategy for digital identity

3) Policy, laws and regulations

4) European Union context

5) Q&A

1

The Dutch identity ecosystem
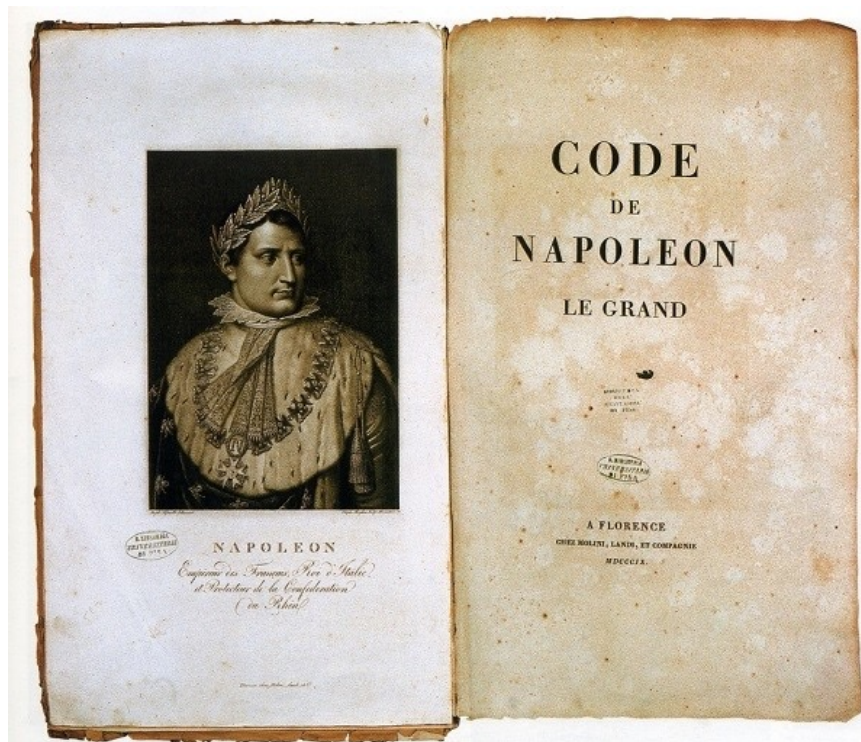
Kingdom of the Netherlands

The Kingdom of the Netherlands is a sovereign state consisting of 4 countries
- the Netherlands
- Aruba
- Curaçao
- Sint Maarten

17.492.000 Million citizens (CBS, 2021-05)

Foundational identity: national population registry and unique identification number

1811: Napoleon introduces first "civil registry" including surnames

1994: Legislation to mandate digitization of population registry

2007: Introduction of the Unique Identification Number (BSN*)

2019: 25th Anniversary of Population Registry (BRP**)
- Over 4,000 connected governmental organisations
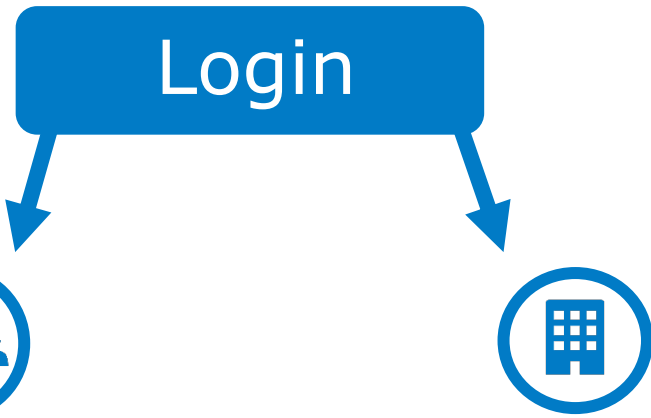- Over 600 Million requests per year

(*) BSN = Burgerservice nummer
(**) BRP = Basisregistratie personen

Recognized identification documents

Authentication to government services

Login

Natural Persons

DigiD

Introduction: 2003

Legal Persons

EHerkenning

Introduction: 2010

Facts & figures 2019

14,7 million
DigiD accounts
(86% of all inhabitants)

341 million
authentications

663
service providers

100 %
availability

7674
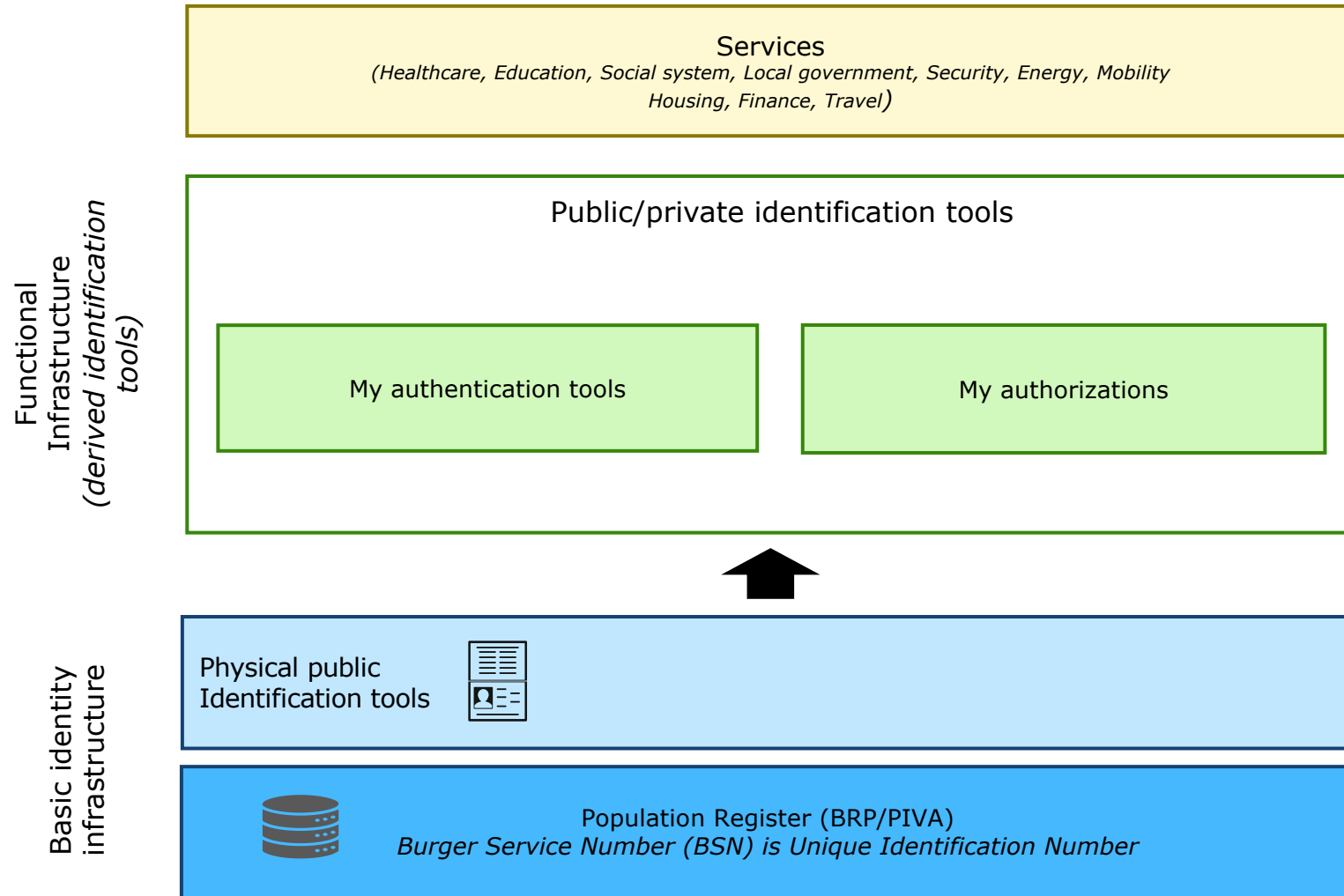highest number of
logins per minute

8,7
user satisfaction
DigiD helpdesk

The existing Dutch ID ecosystem

Services
(Healthcare, Education, Social system, Local government, Security, Energy, Mobility Housing, Finance, Travel)

Functional Infrastructure *(derived identification tools)*

Public/private identification tools

| My authentication tools | My authorizations |

DigiD
EHerkenning

Basic identity infrastructure

Physical public Identification tools

Population Register (BRP/PIVA)
Burger Service Number (BSN) is Unique Identification Number

In a changing world, developments are speeding up

Digitization

➢ Connecting everyone and everything: digital and physical; people, organisations and things;

➢ Growth in digital services and transactions

➢ The coronavirus crisis accelerated the Digitization of services and transactions

Globalisation

➢ Pre-coronavirus crisis: growth in international travel

➢ Pre-coronavirus crisis: rising international migration

➢ The European Union is vigorously pursuing digitization as a catalyst for sustainable growth. The 'Digital Identity' is a major pillar in this pursuit.

Speed of innovation (in relation to policy, laws and regulations)

➢ Dependency on big tech companies

➢ Fragmentation and siloed ID solutions

➢ Complexity for citizens and businesses

Greater dependence on our digital identity infrastructure

➢ Cyber threats and societal risks

➢ ID fraud

Social developments

➢ Privacy

➢ Inclusion

➢ Transparency

➢ The coronavirus era (work from home – social distancing)

Examples of innovations and experiments

- Digitization and automation of processes

- Legislation to support experiments

- Mobile passport / ID card

- eID card / fingerprints

- API based access to population registry

vID: ID van de toekomst

2

Dutch strategy for digital identity

Building trust in the digital world

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk
www.linkedin.com/company/ministerie-van-bzk

Kenmerk

Uw kenmerk

Datum   February 11, 2021
Betreft   Vision on digital identity

Letter from the State Secretary for the Interior and Kingdom Relations to the House of Representatives on the government's vision on digital identity

1. Introduction

I am writing you to inform the House of my vision on digital identity. The purpose of this vision is to set out a clear course on this socially important issue. I shall begin by describing the challenges this issue presents to society. I will then set out my vision and conclude by outlining the international context and suggesting some follow-up steps to take.

It is clear that there are many who feel that a strategic approach to this issue is needed and could prove very valuable.[1] While working on this vision I focused first and foremost on ensuring that it would enjoy broad support, and this has turned out to be the case. The vision has been drawn up in collaboration with a number of ministries, subnational authorities, knowledge institutions, service providers and identity providers. I also received input from international experts in this field. The procedures adopted in drawing up this vision were as transparent as possible, since this is an issue that affects everyone in society.

Goal and parties involved:

To formulate a coherent, shared vision on *digital identity* that takes into account social and political needs, laws and regulations, guiding principles and the existing ID ecosystem.

Ministry of the Interior and Kingdom Relations

The *Digital identity vision: Building trust in the digital world* was realised in collaboration with:

➢ The Ministry of the Interior and Kingdom Relations, Directorate-General Governmental Organization

➢ The Ministry of the Interior and Kingdom Relations, National Office for Identity Data

➢ The Ministry of the Interior and Kingdom Relations, Logius

➢ The Ministry of the Interior and Kingdom Relations, Directorate of Constitutional Affairs and Legislation

Sectoral insights

In addition to various colleagues in the Ministry of the Interior and Kingdom Relations, the parties have consulted the following organisations:

➢ The Association of Dutch Municipalities (municipal domain)

➢ The Ministry of Health, Welfare and Sport

➢ The Ministry of Finance

➢ The Ministry of Economic Affairs and Climate Policy

➢ The Ministry of Justice and Security

➢ Cyber Security Council (cybersecurity)

➢ Schiphol Group (international travel)

➢ International (digital) identity experts

Justification for a 'digital identity vision'

In the digital world, there is a severe lack of trust when citizens and businesses arrange their affairs online with one another or with the government.

Increasing this trust will require a solid framework for our online digital identity, as well as a clear picture of what the role of government should be in relation to the digital identity of Dutch natural persons and legal entities.

Digital identity?

Digital identity

Digital identity can be defined as:

A collection of reliable data that represents an entity (person, organisation, object or device) in the digital domain.

Examples
- Name, date of birth and address
- Static identifying data, identifiers (e.g. UIN, bank account number or telephone number)
- Biometrics (e.g. facial recognition and fingerprint identification)
- Certificates (e.g. diplomas or driving certificate)
- Dynamic attributes, such as digital transactions (e.g. financial)

Delineation

- We are limiting our digital identity vision to natural persons and legal entities.
- The identity of objects and devices will not be considered, although the question of general government policy in these areas will certainly arise at a later stage.

The introduction of foundational digital identity

Digital Base Identity (DBI)

A digital identity for **public and private sector** use that is **government-issued**, recognised and enshrined in a legal and **regulatory framework**.

The DBI contains the **minimum set of identity data** required for societal transactions.

With the DBI, the government is creating an '**authoritative source**' of reliable personal identification data. This will provide an important general building block to foster greater trust in the digital world.

Using the DBI as an 'authoritative source' allows for the use of **derived (secondary) identification tools** and trust services.

See the appendix for a list of terms with definitions

Digital ID vision based on four pillars

1. **Sharing reliable data:** Our vision is based on having the government serve as the 'authoritative source'. Sharing governmental data that have been verified for digital services increases trust in the public and private domain. This is in line with the Dutch Government policy objectives for personal data management and the European ambitions for the Single Digital Gateway.

2. **Access:** The organisation of access to vital services for all citizens and businesses in Dutch society at an appropriate (eIDAS) level of assurance, applicable in both the public and the private domain.

3. **Digital base identity:** A digital identity for public and private sector application that is government-issued, recognised and enshrined in the legal and regulatory framework.

4. **Dutch Digital trust framework:** The basic principles and agreements concerning data sharing, access and fostering trust in the digital world, including the digital base identity (DBI), are governed by a system of agreements titled 'The Dutch Digital Trust Framework (DDTF)' (working title).

The universal guiding principles for a digital identity infrastructure

Inclusion

1. Everyone has a right to a digital base identity. This pertains to legal entities and natural persons who have a relationship with the Dutch government.

2. Obtaining and using a digital base identity is a simple and intuitive process.

3. People who struggle to use digital identification tools can either get assistance or authorise someone to represent them.

4. Government has a duty of care for citizens having problems with their digital identity.

Design

4. The digital identity is intended for use by natural persons and legal entities in the public and private sector.

5. The digital identity infrastructure is robust, transparent, reliable, unique and secure.

6. The digital identity infrastructure adheres to current and future national and international developments and standards.

7. The digital identity infrastructure offers safeguards to protect the privacy of natural persons and legal entities.
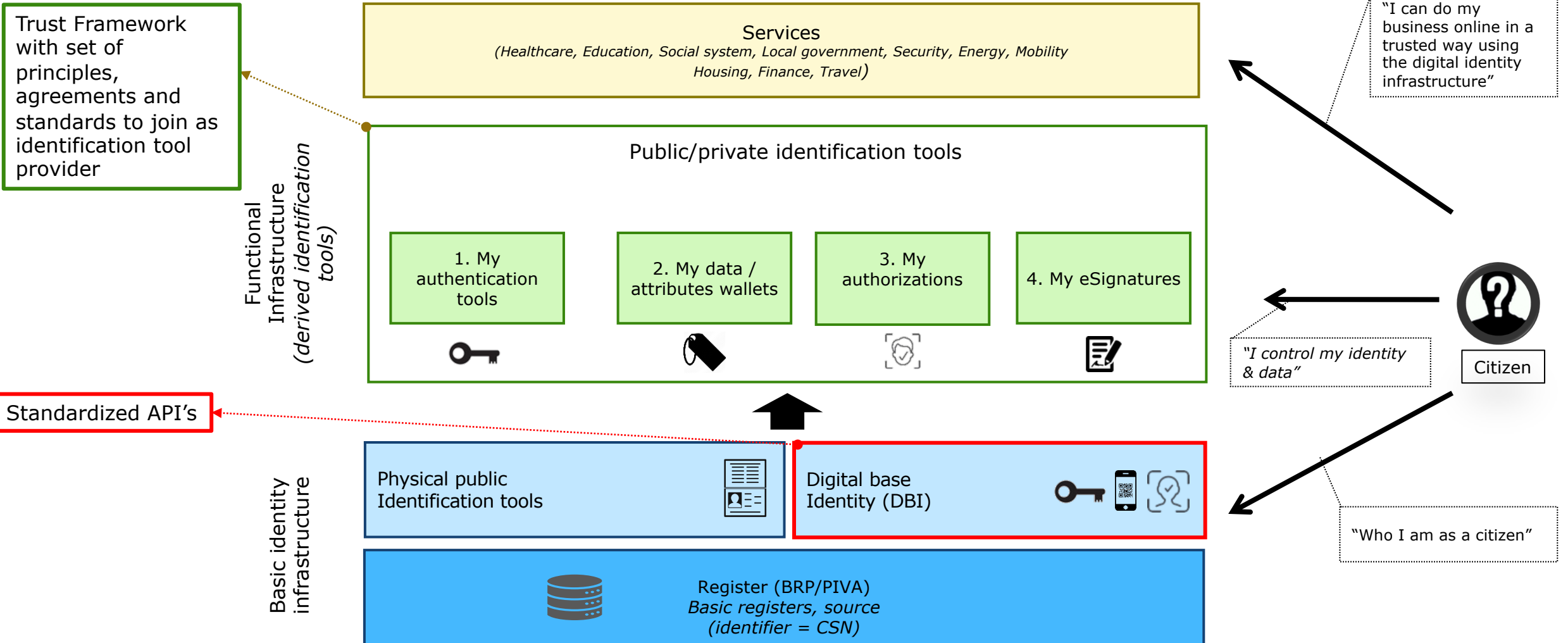
8. Government issues identification tools and admitted (private) identification tools process only the data required (data minimisation) for their operation, whereby there is a legal basis for this action or explicit, voluntary, user (whether a business or a citizen) consent.

9. Regarding the use of the digital (base) identity, there will be room for innovation and opportunities to make individual choices (flexible infrastructure).

Governance

10. The government creates the basic conditions that enable trust in the digital domain.

11. Issuing a digital base identity is government task.

12. The digital identity infrastructure is enshrined within the legal and regulatory framework.

13. There is independent oversight over the use of the digital base identity and the authorised parties in the digital identity infrastructure.

14. As part of digital identity governance, there will be an independent organisation that represents citizens.

The DBI as part of the basic ID infrastructure

Trust Framework with set of principles, agreements and standards to join as identification tool provider

Standardized API's

Functional Infrastructure (derived identification tools)

Basic identity infrastructure

Services
(Healthcare, Education, Social system, Local government, Security, Energy, Mobility Housing, Finance, Travel)

Public/private identification tools

1. My authentication tools	2. My data / attributes wallets	3. My authorizations	4. My eSignatures

Physical public Identification tools	Digital base Identity (DBI)

Register (BRP/PIVA)
Basic registers, source (identifier = CSN)

"I can do my business online in a trusted way using the digital identity infrastructure"

Citizen

"I control my identity & data"

"Who I am as a citizen"

3

Policy, laws and regulations

Challenge in the domain of digital identity

Central issue:

➤ **The central issue is the lack of trust in the digital world**. Increasing this trust will require a solid framework for our digital identity, as well as a clear picture of the role the government should fulfil in relation to the digital identity of Dutch natural persons and legal entities.

What are the social opportunities in the digital identity domain?

➤ Government in the role of an authoriative source of digital identity can stimulate **trust in all transactions in society**
➤ Advancing citizens' **independence** and **autonomy**
➤ Safeguarding the basic right to **privacy**
➤ A robust digital identity infrastructure can boost the Netherlands' (and the EU) **economic position**
➤ A clear and coherent digital identity infrastructure and a good digital signature will help citizens and businesses interact online and **reduce (international) administrative burdens** and unnecessary societal costs.
➤ A clear and coherent digital identity infrastructure will promote **cybersecurity** for citizens and businesses.
➤ By laying a clear foundation for the digital identity infrastructure (e.g. the physical means of identification), **the government can act as a reliable partner** for other parties that wish to innovate in this domain.
➤ **Secure data exchange**, such as in the healthcare sector with patient consent.
➤ A secure, reliable and future-proof digital identity infrastructure can help combat **identity fraud**.

LOGIN
PASSWORD

A A

What is the role of the government?

In a digital identity vision, government is able to have different roles. For each of these roles, we should be explicit about what role the government will have in the future:

➢ Legislator (the guardian of fundamental rights, implemented in part through European legislation and international agreements)

➢ Policy creator (translation of politically determined public values into policy)

➢ Enforcer (The government will need to enforce the repercussions for any policy breaches)

➢ Registrar (registration and storage of elements and/or aspects of an individual's identity, attributes)

➢ Service provider (execution of government services)

➢ (Digital) identification tool supplier (incl. management, request and issuance)

➢ Financier or co-financer of resources or systems

Please note: These roles differ from the traditional public policy context. They have been formulated like this because within the digital identity infrastructure, the roles of the government greatly vary and are partly independent of one another.

Existing legal perspective

Legal means of identification

- **Passport** (travel, identification, nationality)
- **ID card** (identification, travel)
- **Driving licence** (driving competence, identification)
- **Residency documents** (residency status, identification)

Additional relevant laws and regulations

- **GDPR (EU):** The General Data Protection Regulation European regulation, including the Netherlands General Data Protection Regulation Implementation Act (Uitvoeringswet Algemene verordening gegevensbescherming)
- **eIDAS (EU):** A European regulation on electronic identification and trust services for electronic transactions in the European Single Market
- **Digital Government Act (Wet Digitale Overheid, WDO):** Legislative proposal. Currently under revision following several additions by the Dutch Senate after being approved by the House of Representatives.
- **Electronic Administrative Communication Modernisation Act (Wet modernisering elektronisch bestuurlijk verkeer):** As of 2021, citizens will have the right to send electronic messages to administrative bodies.

Identification Requirement Act (Wet op de identificatieplicht, WID)
Designates legal means of identification

Sectoral legislation with identification elements:
- Licensing and Catering Act (Drank- en Horecawet)
- Aliens Act (Vreemdelingenwet)
- The Municipal Personal Records Database Act (Wet basisregistratie personen, BRP)
- Netherlands Electoral Law (Kieswet)
- General Provisions on the Citizens Service Number Act (Wet algemene bepalingen BSN)
- Dutch Criminal Law
- Long-term Care Act (Wet langdurige zorg)
- Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme, Wwft)
- Act on the Notary Profession (Wet op het notarisambt)
- Savings Certificates Act (Wet inzake spaarbewijzen)
- Passenger Transport Act (Wet op personenvervoer)
- Framework Act on Military Service (Conscription) (Kaderwet dienstplicht)
- Law on Plant Protection Products and Biocides (Wet gewasbeschermingsmiddelen en biociden, Wgb)
- Veterans Decree (Veteranenbesluit)
- Participation Act (Participatiewet)
- Dutch Civil Code
- Etc.

Legislative developments in digital government act

Owner		Ministry of Interior and Kingdom Relations
Supervisory body		Radiocommunications Agency
Operational context		Approx.. 700 relying parties
eID schemes		DigiD, eHerkenning Digital Government Act: Open eID scheme
Legal Context		GDPR / eIDAS / WABB / WID / TW / PW Single Digital Gateway / Digital Government Act / Digital Base Identity / Data ownership

Existing policy principles

Existing policy

A digital identity vision touches on a multitude of issues regarding digital government and personal data. This vision builds on the following policy principles:

› Letter to Parliament on the international eGovernment perspective (October 2020) (link)

› Letter to Parliament on the release of source code for governmental software (April 2020) (link)

› Update of the NL DIGITAAL Government Data-Agenda 2020 (March 2020) (link)

› Letter to Parliament about the progress on the approach to digital access (January 2020) (link)

› Letter to Parliament concerning the state of affairs of the BRP (civic) Register (November 2019) (link)

› NL Digibeter, Digital Government Agenda (July 2019) (link)

› Dutch Digitalisation Strategy 2.0 (July 2019) (link)

› Policy letter on further development of personal data management (July 2019) (link)
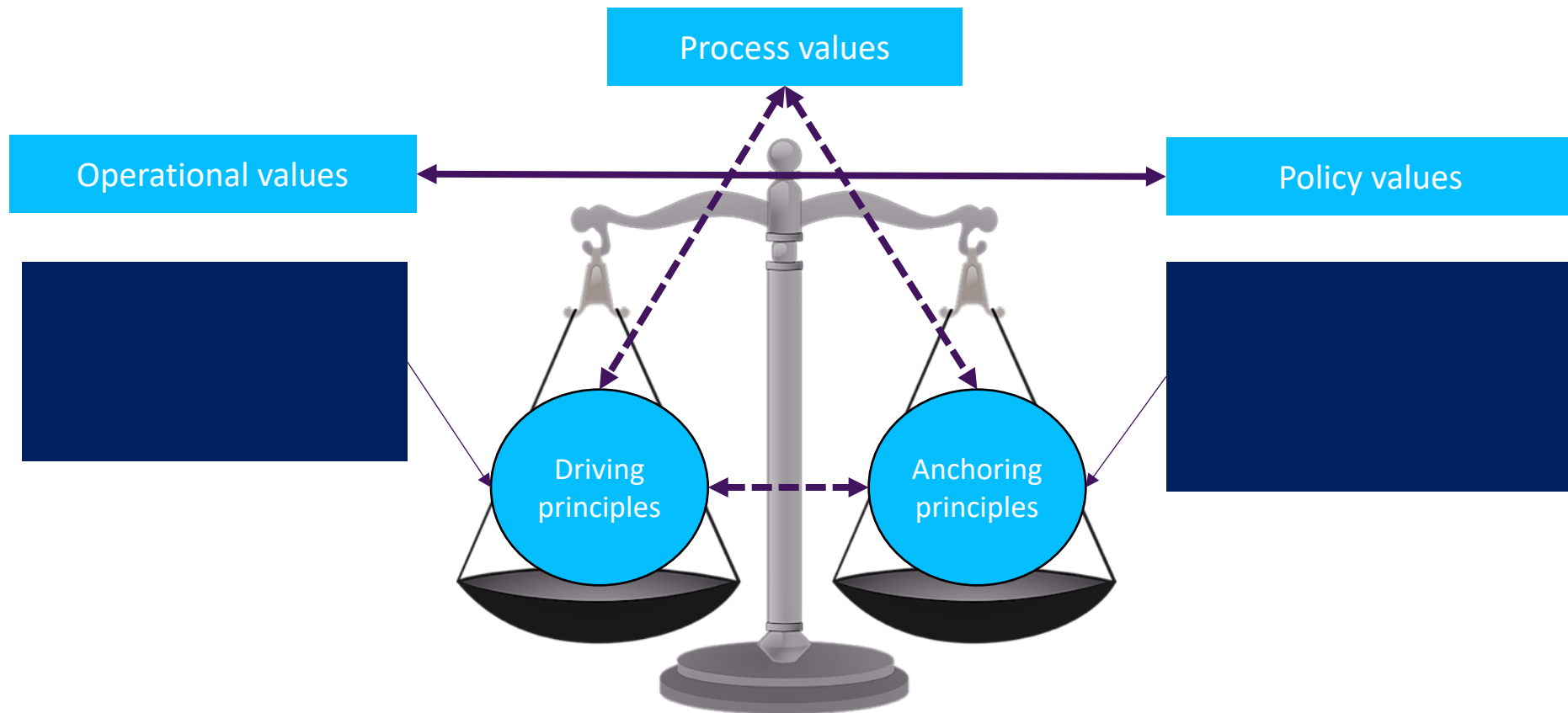
Sorted by publication date

TRUST & LEGITIMACY

1. Accountability
2. Transparency

Process values

Operational values

Policy values

Driving principles

Anchoring principles

Please note: finding the right public value balance is not a zero sum game. In the right balance the weights can be increased.

TRUST & LEGITIMACY

1. Accountability
2. Transparency

Process values

Operational values

Policy values

1. Innovation
2. Effectiveness
3. Efficiency
4. Security
5. Reliability
6. Privacy
7. Autonomy

1. Inclusion
2. Privacy
3. Freedom of Choice
4. Duty of Care
5. Personal Autonomy
6. Safety
7. Equality (of opportunity)

Driving principles

Anchoring principles

Please note: finding the right public value balance is not a zero sum game. In the right balance the weights can be increased.

Policy dilemma:

Do we trust our citizens with their own identity and verified data?

Do we really believe in self sovereign identity?

(duty of care vs. autonomy)

Policy dilemma:

To what extend can our governments function as a public value and rule based platform on which other parties can offer innovative services?

(Government as a Platform)

4

## European Union context

EUROPEAN INNOVATION SCOREBOARD 2019

Innovation Leaders
Strong Innovators
Moderate Innovators
Modest Innovators

eIDAS Regulation on **eID**entities **A**nd trust **S**ervices for electronic transactions in the internal market
(EU 910/2014)

eIDAS
state of play - NL

› # authentications
  – 9000 authentications per month
  – Top 5: taxes, social security, education, fines and pension
  – 243 affiliated organisations

Inkomend eIDAS verkeer uit

Authenticaties en aansluitingen op eIDAS infrastructuur
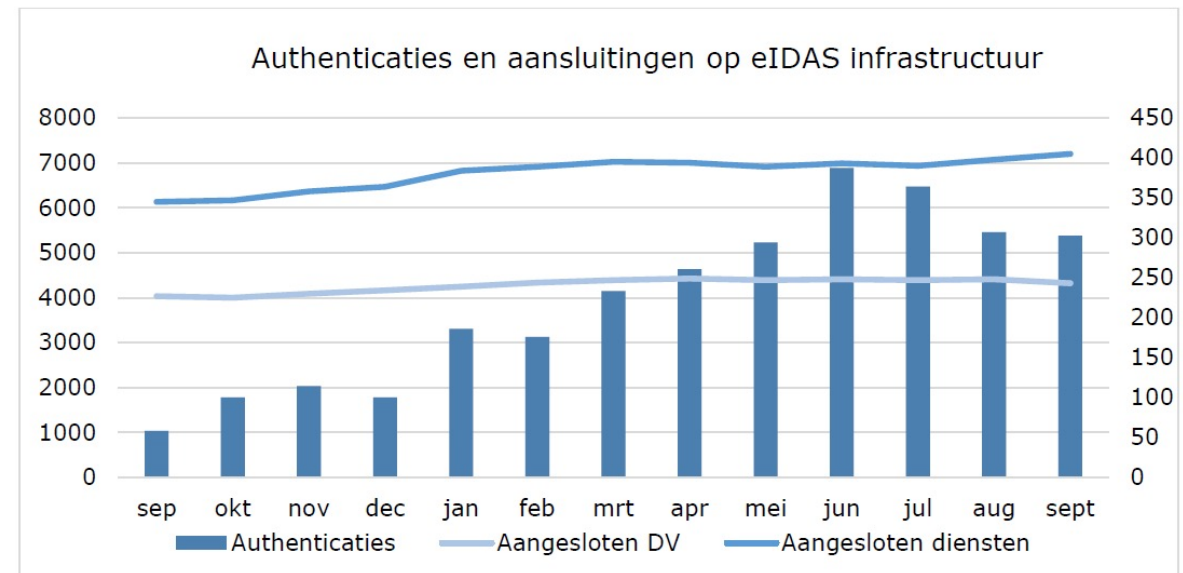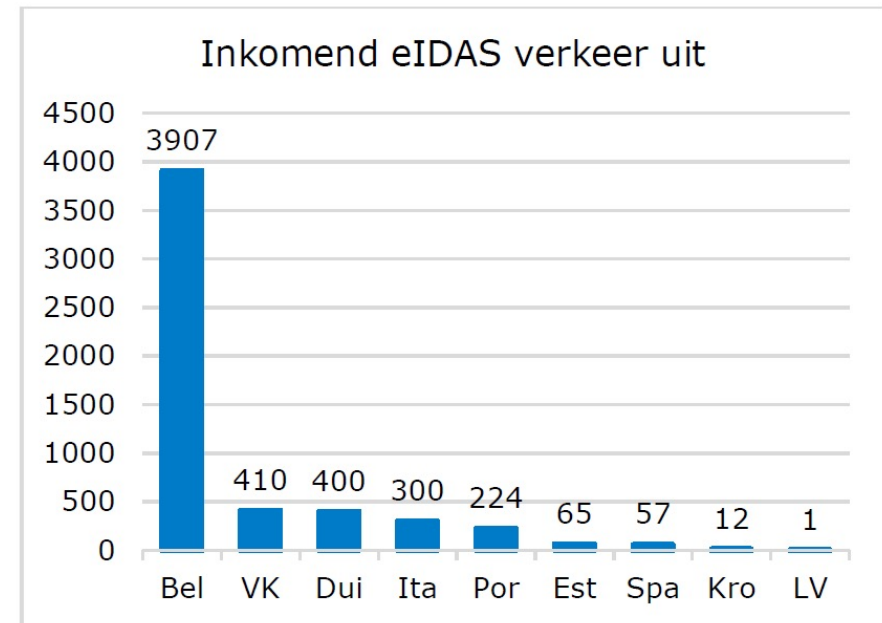
European Commission: improve the effectiveness of eIDAS

Can citizens and businesses really use their national eID for trustworthy cross border identification?

- Only 14+ EU Member States notified

- Only 15% of public services connected

- No services for companies

- High costs per transaction

Improve the effectiveness of eIDAS: option 1

Reinforced Baseline Scenario

- Increase uptake by connecting more services and more eID tools

- Uptake businesses ('legal persons'): re-evaluate, improve the use of mandates within EU

- Guidance on biometrics and remote identification

Improve the effectiveness of eIDAS: option 2

Broaden the scope

- eID tools also for the private sector

- eID tools for devices?

Improve the effectiveness of eIDAS: option 3

European Digital Identity Scheme

- eID tools fitting in one EU eID scheme for al citizens to use in every relevant sector of society

- "Wallet based systems that are quite safe and convenient"

Challenges and opportunities for a public value based eIDAS revision
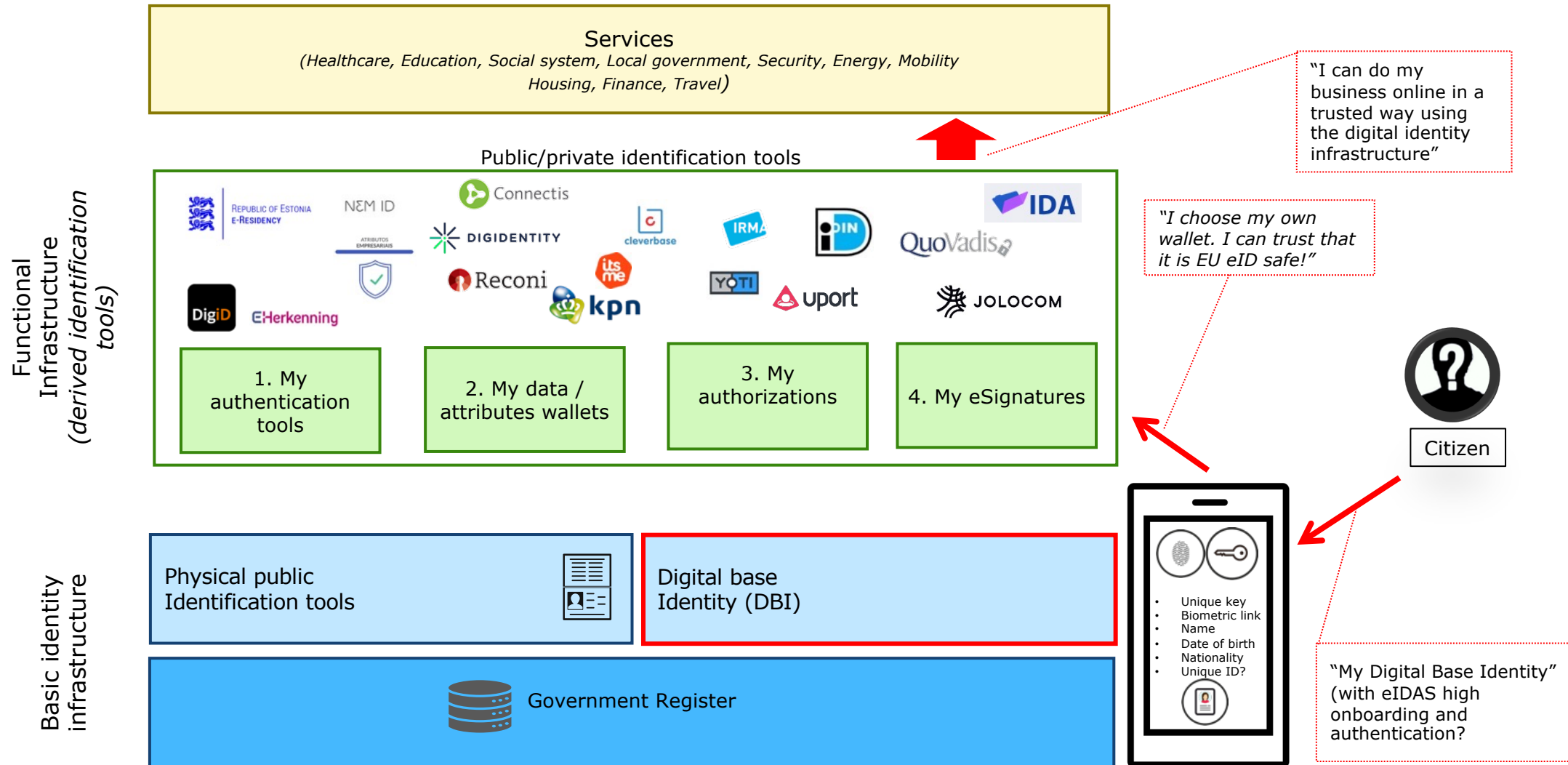
1. **Principle based European eID framework**

    *   EU should set the shared European principles on what is acceptable for eID providers to offer in the EU digital domain. A European eID framework. This is a question of public value and shared human rights.

    *   For example. Principles like:

        *   People who struggle to use eIDs can either get assistance or authorise someone to represent them.

        *   Link to the digital services act: identity data or eID use data can never be used for personalized adds

2. **Can we have shared concept on the financial model behind eIDs?**

    *   There are many funding models of eID scheme's. The Netherlands now has a public issued eID for use in the public sector only. This is collectively funded. How do we expand to the private market with a fair competion in the market?

    *   Will there be cross border competition? And will states join the competition?

        *   Fundiing options:

            1. Government funded

            2. Citizen funded

            3. Verifying party (service provider) fee,

            4. Metadata / cross selling options funded (you are the product)

The DBI as part of the basic ID infrastructure

Services
(Healthcare, Education, Social system, Local government, Security, Energy, Mobility Housing, Finance, Travel)

Public/private identification tools

Functional Infrastructure *(derived identification tools)*

1. My authentication tools

2. My data / attributes wallets

3. My authorizations

4. My eSignatures

Basic identity infrastructure

Physical public Identification tools

Digital base Identity (DBI)

Government Register

"I can do my business online in a trusted way using the digital identity infrastructure"

"I choose my own wallet. I can trust that it is EU eID safe!"

Citizen

- Unique key
- Biometric link
- Name
- Date of birth
- Nationality
- Unique ID?

"My Digital Base Identity" (with eIDAS high onboarding and authentication?

Summary

› **Dutch ID ecosystem:**
The existing Identification system in Netherlands is robust, inclusive, reliable and trusted. Innovations have to be organized within the existing context (no green field)

› **Dutch strategy for digital identity:**
The vision focuses on building trust in the digital world with a foundational digital identity and reliable data sharing (authoritative source of trust model)

› **Policy, laws and regulations:**
The design of policies laws and regulations for our ID system depends also on political choices on how to develop our society

› **European Union Context:**
ID systems have to operate and innovate in the context of cross border identification and trust within the European Union (and beyond). This should be a public values and principle based ID ecosystem.