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.

This letter sets out the strategy for our digital identity and the roles and responsibilities that the government will fulfil in the digital identity infrastructure. It follows up on the recent letters from the government on the subjects of digital inclusion, control of data, digital access and the Digital Government Agenda.[2]

Appendix 1 describes the concepts of digital identity, the digital identity infrastructure and the various functions and roles involved, in order to provide a clear definition of and focus on the issue.

[1] See *inter alia* 'Brede Maatschappelijke Heroverwegingen, Thema 13 Een betere dienstverlening voor Burgers en Bedrijven' (Social Reassessment, theme 13: Better service provision for the public and the business community): Parliamentary Papers, House of Representatives 2019/20, 32359 no. 4.
[2] Parliamentary Papers, House of Representatives 2020/21, 26643 no. 721.
Parliamentary Papers, House of Representatives 2018/19, 32761 no. 147.
Parliamentary Papers, House of Representatives 2020/21, 26643 no. 711.
Parliamentary Papers, House of Representatives 2019/20, 26643 no. 700.

2. Societal challenges and opportunities

Our world is changing rapidly, and many of the changes have an impact on how we manage our digital identity. A digital identity is now a vital way of safeguarding the trust that is so important in all interactions and transactions conducted online without personal contact. Without a reliable system governing our digital identity, it is difficult to trust the person or organisation with whom we are doing business online.[3]

Being able to trust the fact that one is interacting with the right organisation or individual is vital for many processes in society. Consider the growing digitization of many critical processes – from eHealth to online banking, and from online shopping to distance learning – which has been further accelerated by the coronavirus pandemic. All of these processes rely on some form of digital identity.[4] Consider also the internationalisation of transactions and the need to reliably identify yourself, to the extent that it is necessary, in various cross-border online processes. The question that constantly arises is how someone can identify him- or herself without compromising their privacy. Without a certain degree of assurance, there can be no trust when dealing with other parties. We therefore need to build trust in the digital world with a reliable digital identity infrastructure.

Greater dependence on our digital identity infrastructure will bring new challenges in terms of cyber threats and online identity fraud.[5] Today the rapid pace of innovation has made many people dependent on large, non-Dutch tech companies, for lack of any alternative. Too often, what appear to be 'free' services are actually 'paid' for with personal data.

There is now a growing focus on transparency and openness of the technology we use, especially when it concerns technologies we can hardly go without. The pace of innovation has also meant that digital identity tools have become too complex for some groups of citizens.[6] I believe it is vital that we guarantee the inclusion of these groups.

Issues that necessitate a reliable digital identity infrastructure include:

- **Digital inclusion**: A decline in the recognisability, user-friendliness and clarity of processes and identity tools poses a risk to the public. This in turn entails the risk that people with fewer digital skills will not be able to participate fully online.
- **Digital security and reliability**: At the moment, citizens and businesses sometimes perform transactions using a digital identity with an inadequate level of assurance.[7] They also often run the risk that their data

[3] For more information on 'trust online' as the most important motivation for a digital identity infrastructure, see World Economic Forum Community Paper, 'Reimagining Digital Identity: A Strategic Imperative': https://www.weforum.org/whitepapers/reimagining-digital-identity-a-strategic-imperative; McKinsey, 'Digital Identification: A Key to Inclusive Growth': https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

[4] For a summary of the opportunities for society, see World Economic Forum Community Paper, 'Reimagining Digital Identity: A Strategic Imperative': https://www.weforum.org/whitepapers/reimagining-digital-identity-a-strategic-imperative

[5] See, for example, Statistics Netherlands' report on the increase in cybercrime and identity fraud: https://www.cbs.nl/en-gb/news/2020/10/less-traditional-crime-more-cybercrime.

[6] For examples of and progress on digital inclusion, see Parliamentary Papers, House of Representatives 2020/21, 26643 no. 721.

[7] European legislation (eIDAS) distinguishes several levels of assurance for identification. Certain services require a higher level of assurance. See Regulation (EU) No. 910/2014 on electronic identification and

are not adequately secured when they enter into transactions online (whether domestic or international).

- **Future-proof services**: The current identity tools infrastructure will not allow public authorities and businesses to continue providing secure, reliable and future-proof services indefinitely.
- **Economic opportunities**: The Netherlands will miss economic opportunities without a secure, reliable and future-proof way of conducting transactions online. A digital identity infrastructure is a crucial element of this.[8]

I believe these issues present opportunities for the Netherlands to develop a reliable digital identity infrastructure. There are clear opportunities for us to better serve a number of important public values:

- By acting as an authoritative source of a reliable digital identity, the government can increase **trust in digital transactions**.[9]
- Promotion of citizens' **self-reliance and autonomy**.
- Better safeguarding of the fundamental right to **privacy**.
- A robust digital identity infrastructure could enhance the Netherlands' **earning capacity**.
- A clear and recognisable digital identity infrastructure would help the public and businesses engage in online transactions, thus **reducing the administrative burden** and unnecessary costs to society.
- A clear and recognisable digital identity infrastructure would enhance **cybersecurity** for both the public and businesses.
- Laying a clear foundation for the digital identity infrastructure (as with physical proof of identity, such as passports) would make the **government a reliable partner** for other parties seeking to introduce innovations in this field.
- **Secure data exchange** in healthcare, for example, with the consent of the patient.
- A secure, reliable and future-proof digital identity infrastructure could help **combat identity fraud**.

The Netherlands is currently among the countries leading the way in this field, but we can and must improve further.[10] I therefore intend to build trust in the digital world by establishing a reliable digital identity infrastructure.

3. Vision: building trust in the digital world

My vision for digital identity involves joining forces to build trust in the digital world. The public and the business community want to be able to perform online transactions with each other and with the government. In the digital world in

trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910&qid=1612282424576.

[8] In its report 'Digital Identification: A Key to Inclusive Growth' McKinsey cites an economic growth potential of 3%-13% of GDP, assuming a reliable digital identity infrastructure is in place: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

[9] The World Bank and other organisations recommend a strategy whereby the government takes the role of authoritative source in a digital identity infrastructure: World Bank Identification for Development (ID4D) Programme, 'ID4D Practitioner's Guide' (2019): https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[10] EU eGovernment Benchmark 2020: https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2020-egovernment-works-people.

which Dutch people and businesses operate, the government takes an active role in creating trust by enabling careful identification, reliable authentication and verified authorisation. Such trust is essential for social and economic development.

A lack of trust will cause hesitancy among individuals, businesses and authorities when it comes to conducting transactions online and using new services. We must therefore develop a digital identity infrastructure that allows online transactions to take place in a reliable, secure and recognisable way, giving people the opportunity to exercise control over an authoritative source of identity data.

Digital Base identity
This authoritative source will comprise the identity of individuals as determined and registered by the government. I intend to use the concept of a 'digital base identity' (DBI) for this authoritative source.[11] It will be a digital identity issued by the government, which is officially recognised and enshrined in law, for use in the public and private sectors. This digital base identity will include a minimum set of identifying data that are needed in societal transactions.[12] By establishing this digital base identity, the government will create an 'authoritative source' of reliable identifying data for individuals, thus providing an important generic building block for trust in the digital world. The DBI as an 'authoritative source' will provide a basis for other digital identity tools, as is currently the case in the offline world with a physical passport, which can be used as an identity credential at a bank, insurance company or energy company. The idea, therefore, is that the government will provide a basic element, which other parties can use within the framework of the digital identity infrastructure to provide reliable services, all under the control and self-determination of the individual citizen.

The principles I intend to apply to the envisaged digital identity infrastructure are set out in appendix 2. Appendix 3 contains a more detailed description of the digital identity infrastructure, including a diagram.

4. Four pillars

My strategy for digital identity and the related infrastructure is based on four pillars. Activities associated with the first two have already been set in motion. The government plans to step up its activities on the third and fourth pillars.

I. **Sharing reliable data**
The foundation of the vision is based on the government serving as an 'authoritative source'. Sharing data verified by the government in online service provision will create trust in both the public and private domains. This is in line with policy objectives concerning the management of data and EU ambitions to create a Single Digital

[11] In this respect the strategy is in line with the amendment to the Digital Government Act proposed by MPs Jan Middendorp and Kees Verhoeven which would introduce an 'online identity'. I propose making the base identity more manageable than the 'online identity' described in the proposed amendment. I do however support the goals of autonomy, and of access to, correction and sharing of data. See Parliamentary Papers, House of Representatives 2019/20, 34972 no. 20.
[12] The digital base identity differs in this sense from the current DigiD online identity credential. DigiD provides individuals with a means of authentication (log-in tool) with various levels of assurance. It does not currently offer people the possibility of independently and reliably using identifying data (such as given name, family name or date of birth) in various societal processes (both public and private).

Gateway. This pillar tracks the activities in the central government programme ‘Taking Control of Data’ and the EU’s proposed Data Governance Act.[13]

II. **Digital access**
Organising access to digital services in Dutch society for all individuals and businesses at an appropriate (eIDAS) level of assurance, in both the public and the private sectors. This pillar tracks the activities of the digital access programme (previously known as eID).[14]

III. **Digital Base Identity**
A recognised digital identity issued by the government and enshrined in law, for use in the public and private sectors.

IV. **Legislation on digital trust**
Legislation laying down the principles and agreements on the sharing of data, digital access and trust services in the digital world, including the base identity. We will draft the legislation in collaboration with all stakeholder parties, and it will include frameworks for clear governance.

5. International/EU context

At European level, the subject of digital identity has implications for the section of the eIDAS Regulation on electronic identification (eID). I bear primary responsibility for this section.

The eIDAS Regulation of 23 July 2014 (EU No. 910/2014) obliges member states to accept each other’s electronic identification means in cross-border digital services between public bodies and citizens or businesses within a year of them being recognised or notified at European level. Under this Regulation, the Dutch eHerkenning and DigiD systems have been notified for cross-border services, and I have made the necessary technical arrangements for the use of other members states’ electronic identification means in online services provided by public authorities and organisations with a role defined in public law.

The European Commission, who is preparing legislative proposals, is currently reviewing the eIDAS Regulation. Last July the Commission published its roadmap in the form of an Inception Impact Assessment,[15] in which it set out its objectives for enhancing the effectiveness of the eIDAS Regulation, in line with its Strategy on Shaping Europe’s Digital Future,[16] through harmonisation, standardisation and certification. This is designed to broaden the scope of the Regulation to digital services in the private sector and to achieve reliable digital identities and services for all EU citizens. It also includes an outline of plans for a European Digital Identity (euID). As soon as the Commission presents its proposals, the House will be informed. Digital identity is not only a focus of the Commission’s Digital Strategy, but also one of the main focal points of the Coalition of the Willing, in which the Netherlands and Finland are taking the lead on this issue.[17]

[13] Parliamentary Papers, House of Representatives 2018/19, 32761 no. 147.
Parliamentary Papers, House of Representatives 2019/20, 22112 no. 2890.
Proposal for a Regulation on European data governance (Data Governance Act): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767
[14] Parliamentary Papers, House of Representatives 2020/21, 26643 no. 711.
[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-
[16] See https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy
[17] Parliamentary Papers, House of Representatives 2020/21, 29362 no. 288.

6. Next steps

This letter outlines my vision for citizens' digital identity, in line with the arrangements in the Digital Government Act. I have instituted preparations to provide a firm legal basis for this vision, and transform it into detailed policy rules and implementation plans. I have also used the investment budget linked to the Digital Government Agenda to launch a number of pilot projects on the digital base identity.

This letter could potentially guide discussion in the forthcoming Permanent Parliamentary Committee on Digital Affairs.

Appendix 1: Definition and focus

It is worth noting that everyone in the Netherlands actually has several digital identities. Numerous organisations keep records in which individuals are represented by a set of data. However, the government, and my ministry in particular, has a unique role as it validates, creates and updates the identities that are most reliable in societal and legal terms, and links them to identity tools that can be used in the real world.[18] The government is thus the most authoritative source when it comes to identity data that can be used easily and reliably in society.[19]

The concept of digital identity is used in many ways, so I would like to start by clearly explaining how I define this concept. A digital identity is a collection of data that represents an entity (an individual or organisation) in the digital domain. Examples include:

- Name, address, date of birth;
- Static identifiers (e.g. citizen service number, bank account number, chamber of commerce registration number or telephone number);
- Biometrics (e.g. facial recognition or fingerprint);
- Certificates (e.g. school examination and degree certificates, driving licence);
- Dynamic attributes[20] such as digital transactions (e.g. bank records).

This vision confines itself to the digital identity of natural persons.[21] The identity of objects and devices will not be discussed, though the issue of general government policy in these areas will certainly arise at a later stage.

The digital identity stored in government records has implications for many issues associated with our ‘digital identity infrastructure’. By this I mean all the systems, arrangements, (security) standards and services associated with the digital identity of individuals.

There are three functions in a digital identity infrastructure, as shown in the figure below.[22]

[18] The most reliable method of identification available in the Netherlands is the passport. Many other registered identities are based on a person’s passport. Identifying information is recorded in the Personal Records Database (BRP).

[19] When I refer to identity data that can be used easily and reliably in the real world, I mean that, like physical means of identification, they can be used in both the public and private sectors.

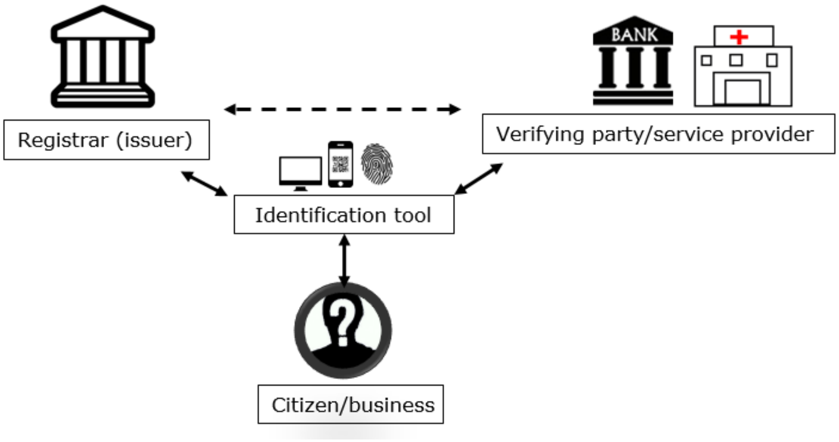
[20] An attribute is a piece of information associated with a certain entity that is registered somewhere. ‘John’ might for example be an attribute associated with a certain entity (an individual). The attribute type is ‘given name’. An attribute is dynamic if its value is mutable. ‘Annual income’ is for example an attribute that can change in value every year.

[21] The identity of legal persons is not considered here, though this strategy certainly has implications on this front, in the sense that a legal person or organisation is always represented by a natural person. The identification, authentication and authorisation functions are also important for this natural person in the context of his/her role in connection with the legal person.

[22] Model from World Bank Identification for Development (ID4D) Programme, ‘ID4D Practitioner’s Guide’ (2019): https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.
Definitions based on the eIDAS Regulation: Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910&qid=1612282424576.

Who are you?	*Are you who you say you are?*	*Are you authorised/eligible?*
Identification	Authentication	Authorisation
Registration of a unique identity (definition and creation) followed by the issuing of an identity credential that allows individuals to have this identity verified.	Process that enables confirmation of an identity, or of the origin and integrity of data in electronic form.	Assessment of whether someone is authorised or eligible to obtain access to a service or information, etc.

In order to properly perform these functions, a digital identity infrastructure defines four roles that can be performed by various parties. These roles are illustrated in the figure below.



Roles in a digital identity infrastructure:

1. Citizen/business: The entity whose data are registered
2. Registrar: The party that registers data in a database and, therefore, is able to serve as an authoritative source
3. Verifying party: the party that wishes to have certain claims verified from an authoritative source to complete and/or participate in an interaction or transaction (service)
4. Identification tool: the party providing the identification tool with which a user digitally makes his or her presence known

The government can assume various roles and responsibilities in a digital identity infrastructure. These future roles and responsibilities are explicitly defined:[23]

- Legislator (the guardian of fundamental rights, implemented in part through European legislation and international agreements)
- Enforcer (compliance with legislation needs to be monitored and enforced)

[23] These roles and responsibilities differ from those in the traditional administrative context. They have been defined as such because in the digital identity infrastructure the roles and responsibilities of the government are performed in a great variety of ways, and exist partly in isolation from each other.

- Registrar (registration and storage of elements and/or aspects of an individual’s identity, attributes)
- Service provider (all provision by the government in the form of services)
- Digital identity provider (plus management, application and issuing process)
- Funder (or co-funder) of identity tools or systems.

Appendix 2: Principles underlying digital identity infrastructure

The envisaged digital identity infrastructure is based on the following principles:

Inclusion

1. Everyone who has a relationship with the Dutch government is entitled to a single digital base identity.
2. Obtaining and using a digital base identity should be a simple and intuitive process.
3. People who experience difficulty using digital identity tools must be able to obtain assistance, or authorise someone else to represent them online.

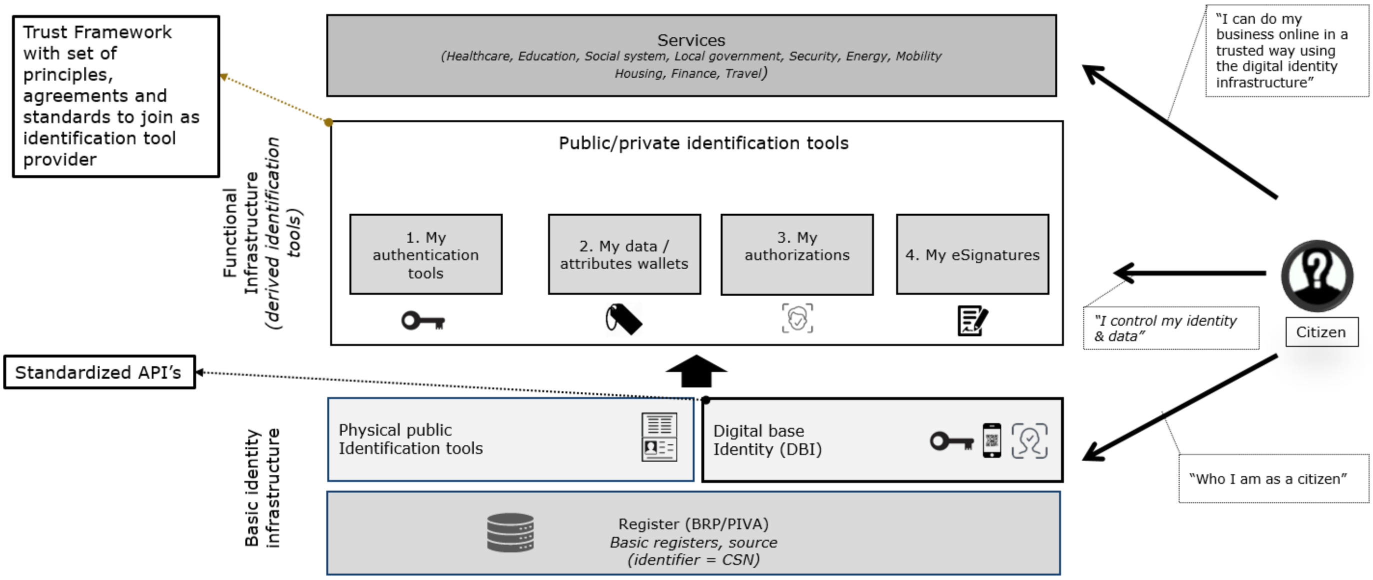
Design

4. A digital identity is intended for use by individuals in the public and private sectors. That digital identity is unique.
5. The digital identity infrastructure must be robust, transparent, reliable, unique and secure.
6. The digital identity infrastructure must be compatible with current and future national and international developments and standards.
7. The digital identity infrastructure and all approved identity tools will guarantee protection of citizens’ privacy (privacy-by-design).
8. There will be a free choice of identity tools and room for innovation in the use of the digital base identity (flexible infrastructure).

Governance

9. The government will draw up the requirements and basic terms and conditions for a secure and reliable digital identity infrastructure.
10. The government will be responsible for issuing a digital base identity.
11. The digital identity infrastructure will be enshrined in legislation.
12. There will be independent monitoring of the use of digital base identities and approved identity tools in the digital identity infrastructure.
13. Digital identity governance will include an independent organisation that represents the public.

Appendix 3: Planned digital identity infrastructure[24]


Trust Framework with set of principles, agreements and standards to join as identification tool provider
Services
(Healthcare, Education, Social system, Local government, Security, Energy, Mobility Housing, Finance, Travel)
"I can do my business online in a trusted way using the digital identity infrastructure"
Functional Infrastructure (derived identification tools)
Public/private identification tools
1. My authentication tools
2. My data / attributes wallets
3. My authorizations
4. My eSignatures
"I control my identity & data"
Citizen
Standardized API's
Basic identity infrastructure
Physical public Identification tools
Digital base Identity (DBI)
"Who I am as a citizen"
Register (BRP/PIVA)
Basic registers, source
(identifier = CSN)

I would like to emphasise three aspects of this infrastructure: the roles and responsibilities of the government, the digital base identity and the principles underlying the digital identity infrastructure.

Roles and responsibilities of the government

- The basic identity infrastructure is the responsibility of the Ministry of the Interior and Kingdom Relations. The infrastructure needs to be generic and sector-independent in terms of its standards and interfaces.
- Members of the public will choose certain tools in the functional infrastructure. The government will provide a framework and monitor the system.
- The government will issue a recognised digital base identity that can be used in both the public and private sectors, and can be used for both civic and commercial purposes. The digital base identity will contain a minimum set of shareable identity data.
- The government will supply a minimum number of generic identity tools in the functional domain. This relates to the rapid pace of change in this domain, which a generic government service cannot match. The aim is to achieve a flexible infrastructure.
- The government will offer standardised interfaces (APIs) that the public can use to add their personal identity data from the digital base identity

[24]
API = Application Programming Interface. A collection of definitions on the basis of which a computer program can communicate with another program.
BRP = Personal Records Database. The Personal Records Database contains personal data on people living in the Netherlands (residents) and people who have left the Netherlands (non-residents).
BSN = citizen service number.
PIVA = Netherlands Antilles and Aruba Personal Information Service. The population register of the Caribbean Netherlands (Bonaire, St-Eustatius and Saba) and the Caribbean countries (Aruba, St Maarten and Curaçao).

to approved digital identity tools (e.g. digital data wallets). This will give people the freedom to choose their functional identity credential.

- The government will develop as few functional digital identification tools as possible. The government supplies the basic authentication tool (DigiD) for access to government services at the required level of assurance (in accordance with the Digital Government Act).
- The principles and arrangements for the sharing of data and provision of trust in the digital world, including digital identities, will be enshrined in legislation, with input from private parties and knowledge institutions.

Digital Base Identity (DBI)

- Every individual will receive a unique DBI that can be used in both the public and private sectors, and in both the civic and the commercial domain. The DBI is a unique digital representation of the government's acknowledgement of your existence, like an ID document in the physical realm.
- The digital base identity will be a generic element of the digital identity infrastructure. It will be as small and as pure as possible in terms of the personal data it includes.
- The digital base identity will make interfaces available to approved parties, including a uniform taxonomy. This will allow people to add their verified personal data to approved identity tools.
- The digital base identity will need to have a high level of assurance so that it can be used in different sectors.
- The digital base identity will have to comply with requirements concerning checks of the physical user and periodic checks of the accuracy of the data.
- Identity tools in the functional ID infrastructure must be compatible with the basic identity infrastructure in the same way that physical means of identification currently also have several functional applications.[25]
- Individuals will be able to see, via their base identity, which authorities are authorised to process their data, check whether the data is correct and, eventually, see which authority has processed their data (single source, once-only principle).[26]

Principles underlying digital identity infrastructure

- The government will allow public and private parties to use personal identifying data – derived from the base identity and/or from a sectoral register – in an identity tool. The parties may be private, semi-public or public, depending on the authorisation framework. Individuals may decide for themselves which functional identity tools they wish to use.
- The government will provide as few functional identity tools as possible. For the time being this will at any rate include the public authentication tool (DigiD) and identity tools necessitated by relevant European and/or international developments and standards.

[25] Central Government. Statutory means of identification: https://www.government.nl/topics/identification-documents/compulsory-identification

[26] The once-only principle is the idea that a person needs to provide their data to the government only once to reduce the administrative burden on citizens and businesses. See https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle
This principle is in line with the objectives of the amendment to the Digital Government Act proposed by MPs Jan Middendorp and Kees Verhoeven: Parliamentary Papers, House of Representatives 2019/20, 34972 no. 20.

- The government will allow various sectors to use various functional identity tools, though the aim will be to define a uniform approval system and monitoring system. Assessment and approval will be administered centrally. Choice of tools will be a sectoral matter.
- The government will organise an open collaborative platform for legislation on digital trust (pillar 4) where providers of identity tools (authorisation, attributes, authentication and signature) can provide input and ideas on the standards, requirements, monitoring and further developments to be set out by the government. Experts from the public and private sectors and academia will also be involved.
- A central regulator will be charged with monitoring compliance with the legislation on digital trust and reuse of identifying data managed by the government in identity tools.
- The government will provide innovation grants for the further development of identity tools within the defined framework.[27]

[27] This will include things like the Digital Government Innovation Budget I recently established. See https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/innovatie/innovatiebudget/ (in Dutch).