Digital Identity Demanding a Lot from DigiD and eHerkenning

2023

Netherlands Court of Audit

Contents

1. Executive summary and conclusions

We have audited DigiD and eHerkenning. These digital authentication services verify whether individuals and businesses are who they say they are. The Minister of the Interior and Kingdom Relations (BZK) is responsible for DigiD and the eHerkenning system. We conclude that DigiD and eHerkenning currently function satisfactorily. We have concerns, however, about the future of digital authentication. The system in place for digital authentication will change on 1 July 2023 when the Digital Government Act (WDO) comes into force. The European Commission has also proposed a Regulation on a European Digital Identity. For security reasons, the only means to log in to DigiD in future will be by app. People with low digital skills will be left even further behind. They, and people with more complex questions, must be represented and assisted in person. There is room for improvement.

Most goals achieved

The original goals of digital authentication have been largely met. We look at 2 of the goals in this summary. The goal of “usage in the Netherlands” has been met. Citizens and businesses are using DigiD and eHerkenning en masse. The “fraud prevention” goal has been partially met. The Minister of BZK does not have appropriate qualitative and quantitative insight into fraud prevention. This is because responsibility for fraud prevention is spread across many organisations.

Benefits weigh up against costs

The benefits of DigiD and eHerkenning seem to weigh up against the costs. A precise calculation cannot be made. The benefits relate chiefly to the time savings gained by the government and society. We found no signs that DigiD and eHerkenning were inefficient.

Satisfactory quality control

In general, the security of IT services and data is under constant threat from the continuous emergence of new challenges. The Minister of BZK has taken appropriate measures to ensure that DigiD and eHerkenning remain available and secure. However, she should better demonstrate that the controls in place for eHerkenning are actually applied in practice. We further conclude that there is too little insight into the total architecture, i.e. the mutual dependence of all components necessary for DigiD and eHerkenning to function correctly. This is particularly important because the system is about to change. Shared insight and oversight are necessary to design the new system and have it function correctly.

Digital Government Act to come into force on 1 July 2023

The system will change as from 1 July 2023 when the Digital Government Act (WDO) comes into force. Other authentication tools will be admitted alongside DigiD and eHerkenning. To enable them, there must be a technical interface that connects all authentication tools. Implementing organisations such as the Employee Insurance Agency (UWV), the Tax and Customs Administration and municipalities will then need to connect to just one central interface. Such an interface is not yet in place.

European digital identity and wallet imminent

If the Council of the European Union and the European Parliament agree, the EU will introduce a European identity. It will take the form of a digital wallet containing proof of identity and other information that citizens and businesses can share with public and private parties. The wallet, like DigiD and eHerkenning, can also be used to log in to services. In the future, many authentications might be made using the wallet and far fewer with DigiD and eHerkenning There is still a lot of uncertainty about the wallet's configuration and how it will fit into the digital authentication system. The wallet must in any event offer the same authentication quality as DigiD and eHerkenning.

Higher assurance levels problematic for people with poor digital skills

Public authorities and their implementing organisations are stepping up their security by introducing ever higher assurance levels. People with poor digital skills are consequently finding it more difficult to use DigiD. Since 1 October 2022, for instance, it has not been possible to log in to the Tax and Customs Administration's *Mijn Belastingdienst* site using only a username and password. An additional check is made by SMS message. Logging in with an SMS code will also be phased out in the future. It will then be possible to log in only by means of the app. This will be difficult for those with poor digital skills, many of whom do not have smart phones or the skills necessary to make full use of them. The Minister of BZK must strike a very fine balance between security and accessibility.

Better support for people with poor digital skills and complex problems

To guarantee accessibility, the Minister of BZK must make digital representation readily available. People with poor digital skills can then authorise a representative to act on their behalf by logging in to a public service using their DigiD account. People can currently authorise a representative at their own request but legal representatives (administrators, guardians or parents) are not allowed to log in on someone else's behalf.

The government also wants to support people with poor digital skills through government helpdesks and has set up Digital Government Information Points (IDOs) in libraries. Digitally-skilled people also need a physical helpdesk if they have complex questions that cannot be answered digitally, such as incorrect entries in fraud registers, gender transition issues, immigration and emigration problems and the like. Besides IDOs, municipal helpdesks could also provide assistance. We found that IDO staff did not have the competences and powers necessary to help the public fully. We recommend that the Minister of BZK determine whether granting IDO staff more powers to help citizens activate and use DigiD accounts would facilitate the further development of IDOs.

2. About this audit

2.1 Why we carried out this audit

The world is digitalising. Citizens, businesses and public authorities are increasingly settling their affairs digitally. Digital authentication – *verification that you are who you say you are* – has already become a prerequisite to access many public services, from COVID-19 apps to electronic tax returns. We audited 2 authentication tools: DigiD and eHerkenning. These are currently the only central authentication tools that citizens and businesses can use to log in to online public services in the Netherlands. We wanted to know:

- whether DigiD and eHerkenning had the right functionalities – such as authorisations – and whether they were continuously available and secure;
- what the costs and benefits of DigiD and eHerkenning were to society;
- whether DigiD and eHerkenning were fit for the future.

Key terms

Digital identity: a set of reliable data that represents a person or organisation in the digital domain.
Identification: the unique denotation of a person or organisation – *who or what is it?*
Authentication: verification of an identity – *are you who you say you are?*
Authorisation: process giving someone access to a particular service or information.

In the Netherlands, there are currently no tools that provide a digital identity as defined above. However, there are digital authentication tools: DigiD for citizens and eHerkenning for businesses. DigiD and eHerkenning are actually services but for the sake of readability, we refer to them in this report as ”authentication tools”.

Authentication laws and regulations will change on 1 July 2023 when the Digital Government Act (WDO) comes into force. The act will allow private authentication tools to be admitted alongside the public DigiD tool. The WDO will also enable businesses to use a public authentication tool alongside the private eHerkenning tool. The latter is laid down in the second part of the act.[1] It is not yet known when this “second tranche” will come into force.

A second major change is a proposal by the European Commission for an EU regulation on electronic identification and trust services (eIDAS2). The effective date of the regulation is not yet known. Under the regulation, every member state must provide a “free” digital wallet containing identification data and other information that citizens and businesses can share with public and private parties. Citizens and businesses will also be able to use the wallet to log in to public services, as they currently can with DigiD and eHerkenning.

2.2 What we audited and how

This section presents our audit questions and explains how we answered them.
A more detailed account of the methodology is provided in appendix 1.

We asked the following audit questions:

1. To what extent have the digital identity goals and the goals for the current DigiD and eHerkenning services been achieved?
We investigated the extent to which usage/adoption, functionality and security goals set by the Minister of BZK since 2013 had been met. To do so, we collected documentation and held interviews.

2. How efficient are eHerkenning and DigiD in comparison with each other and with other authentication tools or comparable services at home and abroad?
We analysed the costs incurred for DigiD and eHerkenning in 2019-2021. We also investigated the potential benefits. To compare the Dutch authentication tools with a foreign authentication tool we circulated a questionnaire to the Supreme Audit Institutions (SAIs) of other European countries.

3. To what extent does the government manage the quality of DigiD and eHerkenning?
We understand quality to mean the availability, integrity and confidentiality of DigiD and eHerkenning: the authentication tools have to work when users need them, the data have to be accurate and only the right persons must be able to access the systems and data.

To answer these questions, we prepared a detailed assessment framework, as shown in § 4.4.1. Assessments were made by means of documentation studies and interviews.

We also investigated DigiD and eHerkenning in the light of the WDO and eIDAS2 by analysing legal texts and documents and holding interviews.

2.3 Organisation of this report

This report comprises the following chapters. Chapter 3 explains how DigiD and eHerkenning work. Chapter 4 answers our audit questions regarding goals, efficiency and quality control. Chapter 5 presents our consideration of the WDO and eIDAS2. Chapter 6 then looks in more detail at the balance between assurance levels and the provision of services to people with poor digital skills.

3. DigiD and eHerkenning

This chapter explains how the DigiD and eHerkenning authentication tools came into being and how they currently work.

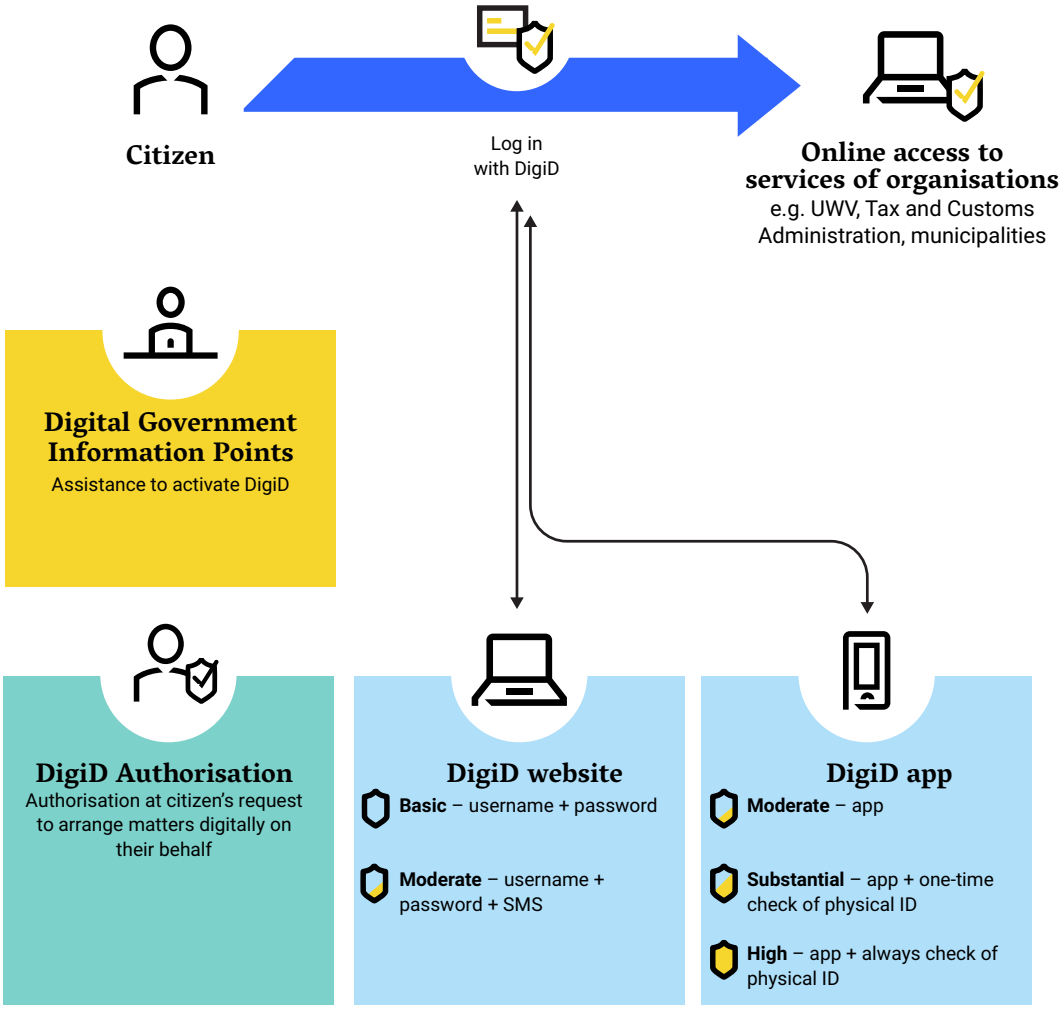
3.1 DigiD

The name DigiD is a contraction of “digital identity”. DigiD was launched by Dutch municipalities in 2003 as a tool to provide municipal information services. The Tax and Customs Administration took over management of DigiD in January 2005, after which it was adopted and used more widely. It is currently managed by Logius, an agency of the Ministry of the Interior and Kingdom Affairs (BZK).

DigiD currently has essentially the same functions as it had in 2003: citizens can log in to DigiD to access online services, and implementing organisations such as the Employee Insurance Agency (UWV), the Tax and Customs Administration and municipalities can verify who is trying to log in. There are several log-in assurance levels, one of which requires use of an app. At their own request, citizens can authorise a person to act on their behalf and can also receive assistance from Digital Government Information Points. This is shown in figure 1.

Figure 1 *Current operation of DigiD*

Citizens can log in to organisations via DigiD



3.2 eHerkenning

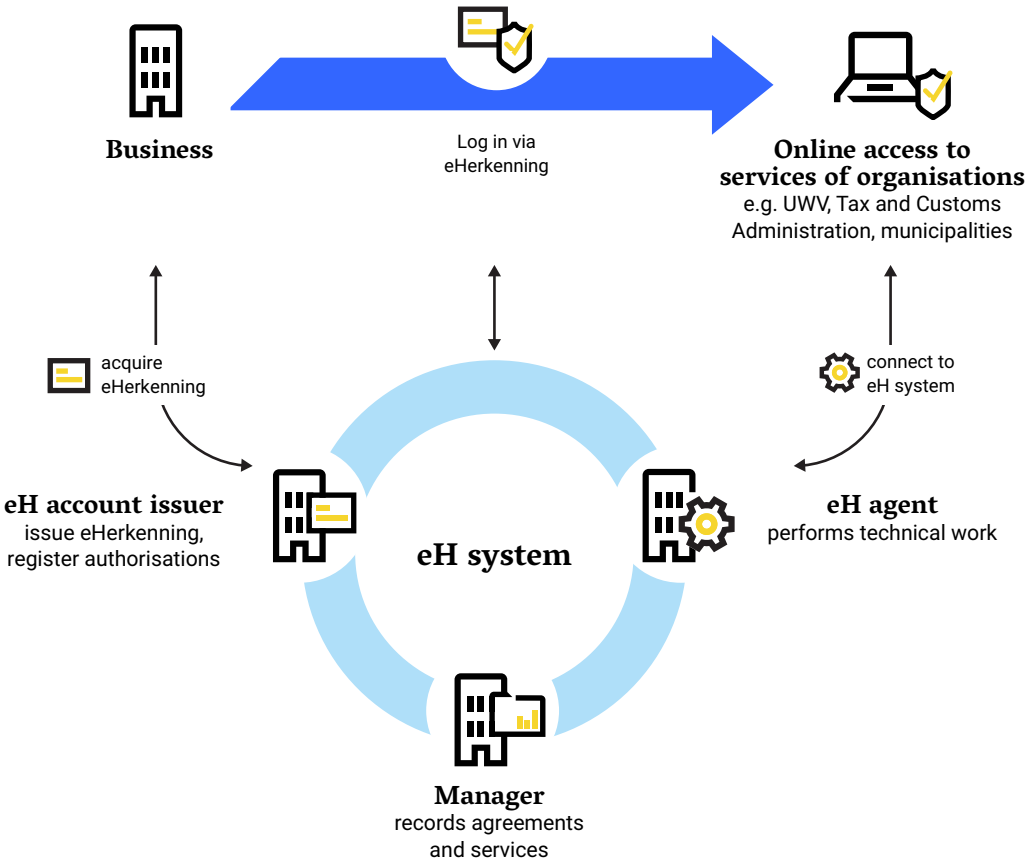
The Minister of Economic Affairs (EZ) developed eHerkenning in collaboration with commercial parties in 2009 as the successor to "DigiD for Business". Before 2009, businesses did not have a reliable and secure online tool to log in to public services. In 2010, NL Agency became the first large service provider to connect to eHerkenning. NL Agency became part of the Netherlands Enterprise Agency (RVO) in 2014.

eHerkenning is a trust framework with a network of public and private parties that provide access services. It is accordingly also known as an electronic access system. The trust framework is available to the public.[2] The framework is shown in figure 2.[3] eHerkenning checks the authentication and authorisation of persons wishing to access an online service. Entrepreneurs can apply to government approved private providers for an eHerkenning account. The figure refers to them as "eH account issuers". Public

authorities can connect to eHerkenning through an eHerkenning agent, also a private party. The trust framework is managed and maintained by Logius, a government agency. One of its tasks is to inform businesses of the services offered by eHerkenning.

Figure 2 *Current operation of eHerkenning*

Businesses can currently log in to organisations via eHerkenning



4. Assessment of DigiD and eHerkenning

In this chapter we assess DigiD and eHerkenning and answer our audit questions.

4.1 Conclusions

The DigiD and eHerkenning digital authentication tools currently function adequately. We base this conclusion on the following findings.

- The goals set by the Minister of BZK for digital identification and authentication in the past 10 years have been largely achieved. We identified usage, functionality and security goals and consider the most relevant ones here. The goal for usage in the Netherlands has been met: citizens and businesses are using DigiD and eHerkenning en masse. One of the functionality goals relates to digital log-ins by legal representatives, such as administrators, guardians and parents. This goal has not been achieved: as yet, a legal representative cannot log in on behalf of, for instance, a person with poor digital skills. The authorisation on request goal has been met. With regard to security, the fraud prevention goal has been partially achieved. Logius has set up an anti-fraud and misuse team but the qualitative or quantitative insight into fraud prevention is unsatisfactory. This is because responsibility for fraud prevention is spread across many organisations.
- The benefits of DigiD and eHerkenning seem to weigh up against the costs. The benefits are chiefly time savings for society as a whole and for the public authorities that provide the services. We found no signs that DigiD and eHerkenning were inefficient. A precise calculation or comparison of the two authentication tools with a foreign authentication tool is not possible because there are too many variables and not enough information is available.

- The Minister of BZK takes appropriate measures to ensure that DigiD and eHerkenning are accessible and secure. However, she should better demonstrate that controls are also applied in practice. Furthermore, in our opinion there is too little insight into the total architecture, by which we mean the mutual dependence of all components necessary for DigiD and eHerkenning to function correctly. This is important because the system is about to change. Shared insight and oversight are necessary to design the new system and have it function correctly.

4.2 DigiD and eHerkenning results

We asked the following audit question: *to what extent have the digital identity goals and the goals for the current DigiD and eHerkenning services been achieved?*
In the past 10 years, the Minister of BZK has set digital identity and authentication goals. We investigated whether they had been met. Below, we indicate to what extent each goal has been achieved. We report only on what, in our opinion, are the most relevant goals. Appendix 2 presents a detailed assessment framework in which we express an opinion on all the goals we examined. The appendix describes the goals and names the sources from which they were taken or derived.

4.2.1 Usage goals

Usage in the Netherlands
The Minister of BZK's objective since 2013 has been to offer tools that enable the government and private parties in the EU to interact and provide digital services. We found that this goal had been largely achieved, given the number of digital services offered by DigiD and eHerkenning. Both public parties (such as the UWV, Tax and Customs Administration and municipalities) and private parties with a public task (such as pension funds and insurers) offer their services via DigiD or eHerkenning. In 2021, 735 organisations provided their services via DigiD, and DigiD itself had 16.5 million active accounts.[4] In the same year, 537 organisations offered their services via eHerkenning and there were 767,700 eHerkenning accounts.[5] Some service providers offer more than one service. The Netherlands Enterprise Agency (RVO), for instance, provides field registration services to farms, innovation credits to entrepreneurs and a range of grant schemes via eHerkenning. The tables below present key data for 2018-2021.

Table 1 *Key data, DigiD (ICTU, 2022)*

	2018	2019	2020	2021
Connected organisations	647	663	701	735
Number of services	945	1,023	1,124	1,457
Active accounts	13,772,269	15,023,119	18,320,835	16,515,691[6]
Authentications	307,956,118	340,758,404	402,519,872	557,008,812

Table 2 *Key data, eHerkenning (ICTU, 2022)*

	2018	2019	2020	2021
Connected service providers	403	443	493	537
Number of services	1,383	1,686	1,927	2,083
Number of organisations with eHerkenning	226,504	276,953	526,643	692,041
Number of eHerkenning tools/accounts issued	285,969	383,994	609,387	767,700
Number of authentications	5,499,618	9,160,456	15,499,531	16,973,001

Usage in the EU

The Minister of BZK also set goals for log-ins from other EU countries via the eIDAS network. We consider this further in § 5.3.1. DigiD accountholders in other EU countries can log in to connected service providers such as municipalities and the national tax authority via eIDAS, and vice versa. German nationals, for instance, can use their log-in tools to access the Dutch Tax and Customs Administration.

The number of EU transactions is lower:

- *Incoming traffic from the EU*: in October 2022, 275 Dutch public service providers or service providers with a public task were connected to the eIDAS network, providing 390 services in total. The total number of incoming authentications in the same month was 10,242.
- *Outgoing traffic to the EU:* this number is even lower: 4,263 transactions. There is no clear picture of how many public organisations and/or organisations with a public task must still connect to the eIDAS network. We could not establish whether citizens and businesses from the Netherlands could make the same transactions via eIDAS as citizens and businesses in other EU countries could. We also found no specific goal for such transactions. The low number of transactions is one reason that eIDAS was revised and eIDAS2 has been introduced.

Mobile usage

Another usage goal is that the authentication tools can be used on mobile devices. DigiD has met this goal. However, it only works on the Google and Apple platforms and citizens are required to register with Google or Apple. If SMS messaging is eventually phased out, all citizens will have to log in via the app. See § 6.2 for more details. eHerkenning has partially met the goal: not all eHerkenning providers currently offer apps.

Accessibility

DigiD and eHerkenning must be accessible. Citizens and entrepreneurs with a visual disability for instance must also be able to use the authentication tools, with assistance if necessary. Not all features of DigiD or eHerkenning are fully accessible. This goal has therefore been achieved only partially.

Assurance levels

Both DigiD and eHerkenning meet the goal of having a series of assurance levels. The levels reflect the classification of the data and the nature of the services accessed. We consider assurance levels in detail in § 6.2.

4.2.2 Functionality goals

The minister has set several goals regarding the functionality of the authentication tools, such as verifying an identity, confirming authorisations, permitting representation and enabling digital declarations of intent and digital signatures.

Identity verification

The identity verification goal has been achieved. Citizens and businesses can use the DigiD and eHerkenning authentication functions to identify themselves for digital services. The tools verify the identity of citizens and businesses.

Authorisation and representation

DigiD has not achieved the authorisation and representation goal in full, but eHerkenning has. Citizens can use DigiD to access public services for themselves or on behalf of someone else if authorised to do so. To this end, DigiD has a DigiD Authorisation function to authorise someone to access 1 specific service for or on behalf of another person. A single person cannot be authorised to access all services.

In some cases, it would seem logical for legal representatives to be authorised to access all services via their own DigiD account on behalf of someone else. The legal representative could be a guardian acting on behalf of a child or on behalf of an

incapacitated relative. Trials are currently being held to enable this but they will probably not be completed for several years. This goal has therefore not been met. For more information see § 6.3.2.

Businesses and organisations use eHerkenning to log in to public services. Businesses must name the persons who can log in on their behalf. This is known as vertical authorisation. If another organisation or business needs to act on someone's behalf, it can do so by means of chain authorisation.

A person can therefore be legally represented in eHerkenning but not yet in DigiD. We consider this further in § 6.3.

Declaration of intent and digital signature
This goal has been achieved. Citizens and businesses can confirm a declaration of intent and agree to the substance of a transaction by means of DigiD and eHerkenning. Digital tax returns, for instance, can be filed with a DigiD signature. Under EU law and regulations,[7] however, qualified electronic signatures cannot be set using DigiD or eHerkenning, but they can by means of other tools offered by private parties.

4.2.3 Security goals

In our IT audit – see § 4.4 – we investigated whether DigiD and eHerkenning took sufficient account of information security to protect the data of citizens and businesses. We consider one of the minister's goals in this section: authentication tools must prevent identity fraud and improper use.

Logius has set up an internal Fraud and Misuse team for DigiD. Fraud reports are also dealt with through the following channels:

- National Ombudsman;
- National Fraud Helpdesk;
- Central Identity Theft and Error Reporting Centre (CMI);
- Logius Helpdesk/Customer Contact Centre (KCC).

eHerkenning does not have an overarching organisation to deal with fraud reports and there is no central helpline to report fraud.[8] The system is designed so that significant cases of potential identification misuse can generally be allocated centrally to the relevant parties. Reporting and responding to specific warnings and reports, however, are decentralised at the organisations themselves, the suppliers and/or service providers.

We found that fraud prevention and response involving both DigiD and eHerkenning were spread across several parties. Qualitative and quantitative oversight is accordingly poor. This harbours the risk that cases are not coordinated and fraud prevention is less effective. The goal of preventing identity fraud has therefore been achieved only partially.

4.3 Costs and benefits of DigiD and eHerkenning

We asked the following audit question: *how efficient are eHerkenning and DigiD in comparison with each other and with other authentication tools or comparable services at home and abroad?*

We cannot say how efficient the authentication tools are but we can say that we found no signs that DigiD and eHerkenning were inefficient. A precise calculation cannot be made, nor can a comparison of the two tools with a foreign authentication tool. There are too many variables and not enough data is available. It is plausible, however, that the benefits of DigiD and eHerkenning weigh up against the costs.

4.3.1 Costs

The total cost to society of DigiD and eHerkenning cannot be calculated. To do so, we would need to know all the connection costs incurred by the implementing organisations, such as the UWV, Tax and Customs Administration and municipalities. We would also need to know how much effort citizens and businesses took to activate an account. This information is, at best, only partially available. We therefore confine ourselves to known costs that are directly related to the development, management and operation of DigiD and eHerkenning.

The direct cost[9] of DigiD to the government in 2018-2021 was:

Table 3 *Cost to central government for the development, management and operation of DigiD (BZK, 2019, 2020, 2021a and 2022a)*

	2018	2019	2020	2021
Development, management and operation	€34,124,000	€28,567,000	€32,218,000	€46,240,000

The table shows that the costs were similar in 2018, 2019 and 2020, but sharply higher in 2021. The higher costs were due chiefly to the COVID-19 pandemic. DigiD was used as a log-in tool to plan corona tests and access test results (BZK, 2022a). The Ministry of BZK finances these costs. It also makes an annual contribution to the

Ministry of Foreign Affairs (BZ) and municipalities to cover the cost of providing DigiD abroad and to non-residents in the Netherlands. In 2021, this contribution amounted to €435,000.

The direct cost to the government of DigiD Authorisation in 2018-2021 was:[10]

Table 3 *Cost to central government for the development, management and operation of DigiD Authorisation (BZK, 2019, 2020, 2021a and 2022a)*

	2018	2019	2020	2021
Development, management and operation	€11,053,000	€12,772,000	€14,215,000	€17,449,000

The direct cost to the government of eHerkenning in 2018-202 was:

Table 4 *Budgeted cost to central government for the development, management and operation of eHerkenning[11] (Logius.nl)*

	2018	2019	2020	2021
Development, management and operation	€3,016,000	€3,600,000	€3,786,000	€3,961,000

The Ministry of BZK also makes a financial contribution for the supervision of the eHerkenning system. These costs exceed €1.5 million per annum.

A straightforward comparison of the cost of DigiD and the cost of eHerkenning cannot be made. The cost of issuing DigiD accounts is included in the costs shown above. eHerkenning accounts are issued by private parties and we have no access to their financial records. However, we estimated the cost in 2021 at about €20 million.[12]

The costs of comparable tools abroad are even more difficult to calculate. This is because of the significant differences in their functionalities. There is also no effective insight into their costs. Only 1 country (Latvia) has data on the past 4 years and a tool (eParaksts) that is more or less comparable with DigiD. This tool costs about €2.5 million a year.[13]

Depending on what is included in the calculation, the total cost of DigiD, DigiD Authorisation and eHerkenning, as presented in this section, is roughly €100 million per annum. This should be borne in mind when reading the following section.

4.3.2 Benefits

The benefits of the *entire digital services system* probably weigh up against the costs. The benefits, too, are difficult to attribute to the individual tools. Log-ins are impossible without DigiD and eHerkenning. These authentication tools are prerequisites and a major source of the benefits of digital services.

Digital services save citizens, businesses and implementing organisations time. We have no insight into the time saved by the businesses and organisations. We can conclude from comparable studies that a digital transaction with the government saves citizens 15 minutes' time on average (Ecorys, 2016 and 2018). At an average hourly salary of €24, this is equal to €6. More than 550 million transactions were conducted via DigiD in 2021.[14] It would be too simplistic to multiply these numbers together, if only because authentication is just one aspect of an overall transaction. We think it is very likely, however, that the benefits do weigh up against the costs. In addition, digital transactions have considerably lower paper and transportation costs.

If the "central" DigiD and eHerkenning authentication tools did not exist, services and sectors would have to find another way to verify the identity of citizens and businesses, for instance by developing their own authentication tools. The costs and security risks would then be higher. Using DigiD and eHerkenning to verify that someone is who they say they are reduces the risk of identity and other fraud and the risk of revealing sensitive personal information, e.g. in the healthcare sector (Ecorys, 2023).

Furthermore, by facilitating digital authorisation on request, DigiD increases the likelihood that grants and social benefits are paid to the right person. The use of social benefits by entitled citizens is also an advantage. An effective digital authorisation procedure also promotes inclusivity. If citizens are incapable of representing themselves, they can authorise someone else to attend to their digital needs (Ecorys, 2018).

4.4 Quality of DigiD and eHerkenning

We asked the following audit question: *to what extent does the government manage the quality of DigiD and eHerkenning?*

The government adequately manages the quality of the authentication tools. This conclusion is based on an extensive IT audit we carried out. The audit assessed the management measures at detailed level as effective, not effective or partially effective.

4.4.1 Audit findings

As noted in § 2.2, we understand quality to mean the authentication tools' availability, integrity and confidentiality:

- *Availability:* are DigiD and eHerkenning available, do they work when they are needed?
- *Integrity:* are the data correct, do they include errors?
- *Confidentiality:* can only the right people access the systems and data?

Components audited

We audited the components of the IT landscape necessary to access and provide DigiD and eHerkenning's services. DigiD's core functionality is *DigiD Kern*. It is responsible for the technical authentication of a person on behalf of an implementing organisation such as the UWV, Tax and Customs Administration and municipalities. eHerkenning's core functionality is an XML aggregator, that part of the trust framework managed centrally by Logius. This is the interface between the trust agreements and the services. The output is the services catalogue. The catalogue informs the parties in the system what agreements and services are available.

Both DigiD and eHerkenning are connected to the BSN polymorphic pseudonym register (BSNk PP). Polymorphic pseudonyms are a technical means to use a pseudonym rather than a citizen service number (BSN). They increase privacy/data protection. BSNk PP will be a key interface in the new authentication system when the WDO comes into force. Every provider of authentication tools must connect to it in the future. This is why we audited this component of the system.

Controls

A control is a procedure to mitigate risk, for example, by making back-ups and responding effectively to security incidents. Controls contribute to availability, integrity and confidentiality. Controls that are relevant to these properties are marked with an "x" in table 6. For the 3 named components (DigiD Kern, eHerkenning, BSNk PP), we audited an extensive set of controls to determine whether they were effective, partially effective or not effective.

- A control is effective if it can be satisfactorily demonstrated that it has been implemented in full. In other words, the control is not only worked out on paper but the auditee can also demonstrate that it is applied in practice.
- A control is partially effective if:
  - only a description of the control is available but there is no evidence that it is applied in practice;
  - a control is applied in practice but has no formally approved description.
- A control is not effective if there is no description and no evidence that it is applied in practice.

The audit findings are summarised in table 6. We state per component and per control whether quality is satisfactorily controlled.

Table 6 *IT audit findings*

				eHer-kenning	DigiD Kern	BSNk PP
	Availability	Integrity	Confidentiality	Controls	Controls	Controls
IT Governance						
Clearly defined roles and responsibilities for service availability	x			Effective	Effective	Effective
Clearly defined roles and responsibilities for security and information security		x	x	Effective	Effective	Effective
Contracting authority/manager can manage effectively through steering information provided systems/processes	x	x	x	Effective	Effective	Effective
Product (Asset) owner is responsible for appropriate maintenance throughout the assets' lifecycle	x			Partially effective	Partially effective	Effective
Organisation and Processes						
Information is classified in accordance with legal requirements, by value, importance and sensitivity and in accordance with specific risk assessment			x	Effective	Effective	Partially effective
There is a screening policy when entering employment and when changing positions			x	Effective	Effective	Effective
Outsourcing						
There is a formally approved outsourcing policy	x	x	x	Effective	Effective	Effective
Outsourcing is monitored in accordance with agreements	x	x	x	Effective	Effective	Not effective
IT Architecture						
There is up-to-date insight into the IT landscape, including the relationships and mutual dependencies of the main components	x	x	x	Partially effective	Partially effective	Partially effective
Interfaces are maintained and implemented in accordance with a for-malised process	x			Partially effective	Partially effective	Effective
Business Continuity						
Continuity plan: information processing facilities have sufficient redundancy	x			Effective	Effective	Effective
Continuity plan: information security is guaranteed during incidents	x			Effective	Effective	Effective
Back-up: of information, software and system diagrams in accordance with back-up policy	x			Effective	Effective	Effective

				eHer-kenning	DigiD Kern	BSNk PP
IT Operations						
Incident management process present	x			Effective	Effective	Effective
Change management: changes in accordance with a formal authorisation and testing process	x	x	x	Partially effective	Effective	Partially effective
Patch management: patch policy applied in practice				Effective	Effective	Effective
System development: formalised method for software development and software implementation	x	x	x	Effective	Effective	Effective
Password management for non-personal admin accounts	x	x		Partially effective	Effective	Effective
Password management for trusted networks or two-factor authentication applied	x	x		Partially effective	Effective	Effective
Access management: rights applied on 'must have' basis		x	x	Partially effective	Effective	Effective
Access management: accounts with elevated rights limited and justified wherever possible		x	x	Partially effective	Effective	Effective
Access management: always personal accounts		x	x	Partially effective	Effective	Effective
Access management: end users have no direct access to, e.g., database		x	x	Partially effective	Effective	Effective
Access management: periodic evaluation of access rights		x	x	Partially effective	Effective	Effective
Component security: up-to-date insight into infrastructure security	x	x		Partially effective	Partially effective	Partially effective
Capacity management: the IT service can bear the regular activity and recover on timely basis	x			Partially effective	Effective	Effective
Logging: of events concerning, e.g., user activity, exceptions and information security incidents		x		Partially effective	Partially effective	Effective
Logging: protection of information from forgery and unauthorised access		x	x	Partially effective	Partially effective	Effective
Logging: of IT maintenance staff and operators, protecting and regularly assessing the log files		x		Partially effective	Partially effective	Effective
Information Security						
Security by design as accepted principle to develop and design systems	x		x	Partially effective	Partially effective	Effective
Detection of and response to security incidents in accordance with formalised procedure	x		x	Effective	Effective	Effective
Vulnerability management: independent periodic test of technical security measures			x	Partially effective	Effective	Effective

			eHer-kenning	DigiD Kern	BSNk PP
Vulnerability management: timely patching of components of the IT architecture		x	Partially effective	Effective	Effective
Standards: maintaining security of information that is exchanged, internally and externally	x	x	Partially effective	Partially effective	Partially effective
Encryption: policy in place on the use of cryptographic management measures	x	x	Partially effective	Partially effective	Effective
Encryption: policy on the use, protection and lifecycle of cryptographic keys	x	x	Partially effective	Partially effective	Partially effective
Personal Data					
There is a data processing register that can be inspected		x	N.A.	Effective	Effective
Data protection impact assessment and regular updates		x	N.A.	Partially effective	Effective
Data minimisation, the collection of the fewest possible personal data		x	N.A.	Effective	Effective
Processing and accountability principles are registered		x	N.A.	Effective	Effective
Incidents with potentially significant consequences are reported	x		N.A.	Effective	Effective

We found that most of the controls to protect the quality of DigiD were effective. Many controls in the eHerkenning IT Operations and Information Security clusters were only partially effective: processes and procedures had been worked out but their application could not be demonstrated in practice. The Minister of BZK must better demonstrate that the measures in place for eHerkenning are also applied in practice.

One control in place for BSNk PP – Logius's outsourcing of activities to ICTU (ICT implementing organisation) – is not effective. ICTU, a government consultancy and project organisation, is responsible for developing the BSNk. There is no description of the work on BSNk PP that it performs on behalf of Logius. The documentation provided therefore does not include formal agreements.

A concise, uniform description of DigiD's IT landscape is not available. Several visual representations were provided by various organisations, such as BZK, Logius and Capgemini, but they are inconsistent. The mutual dependence of the eHerkenning components was unclear. The available reports could not always be matched one-to-one to specific components. In the case of BSNk PP, the IT architecture diagrams have not been updated since 2018. This entails the following risk. Changes to one IT component can affect an adjacent component. If it is not known which components are affected, there can be consequences for the IT service.

We found that the IT architecture for both DigiD and eHerkenning was neither up to date nor consistent. We had expected more clarity regarding how all IT components worked with each other. We did not gain a proper insight into the IT underlying the authentication service. This is important chiefly from the external perspective of, for instance, a member of parliament or a supervisory or audit organisation. If the mutual dependence of components is known, service provision and IT changes can be managed more efficiently. Shared insight and oversight are also necessary to design and operate the new authentication system under the WDO.

5. Digital Government Act and European digital identity

5.1 Conclusions

- The Digital Government Act (WDO) will change the digital access system as from 1 July 2023. Other authentication tools will be admitted alongside DigiD and eHerkenning. A technical interface is therefore required to connect all the authentication tools. Implementing organisations will then need to connect to just one central interface. Such an interface is not yet in place.
- A European digital identity is also being prepared. Known as the “wallet”, this digital folder will contain identity data and other information that citizens and businesses can share with public and private parties. Citizens and businesses can also log in to implementing organisations via the wallet, as they currently do via DigiD and eHerkenning. In the future, many authentications might be made via the wallet and far fewer via DigiD and eHerkenning. The wallet must offer the same authentication quality as DigiD and eHerkenning. There is still a lot of uncertainty about the wallet’s ultimate configuration and how it will fit into the digital authentication system.

5.2 Digital Government Act

The Digital Government Act (WDO) was first proposed in 2016. Under its initial name, the Generic Digital Infrastructure Act (GDI), it was the subject of internet consultation. Following amendment, the WDO was passed by both houses of parliament in spring 2023. It will come into force on 1 July 2023. The WDO comprises the act itself and a series of secondary decrees and regulations.[15]

The WDO lays the foundations for the further digitalisation of government. It will standardise the authentication system wherever possible. The act contains rules on security and security control. It also regulates citizens' and businesses' digital access to public services. It includes rules on secure log-ins to access government and semi-government services. Figure 3 shows the main changes that the WDO will bring about in the authentication system.

Figure 3 *Access system when the WDO comes into force*

Introduction of the WDO will change the authentication system

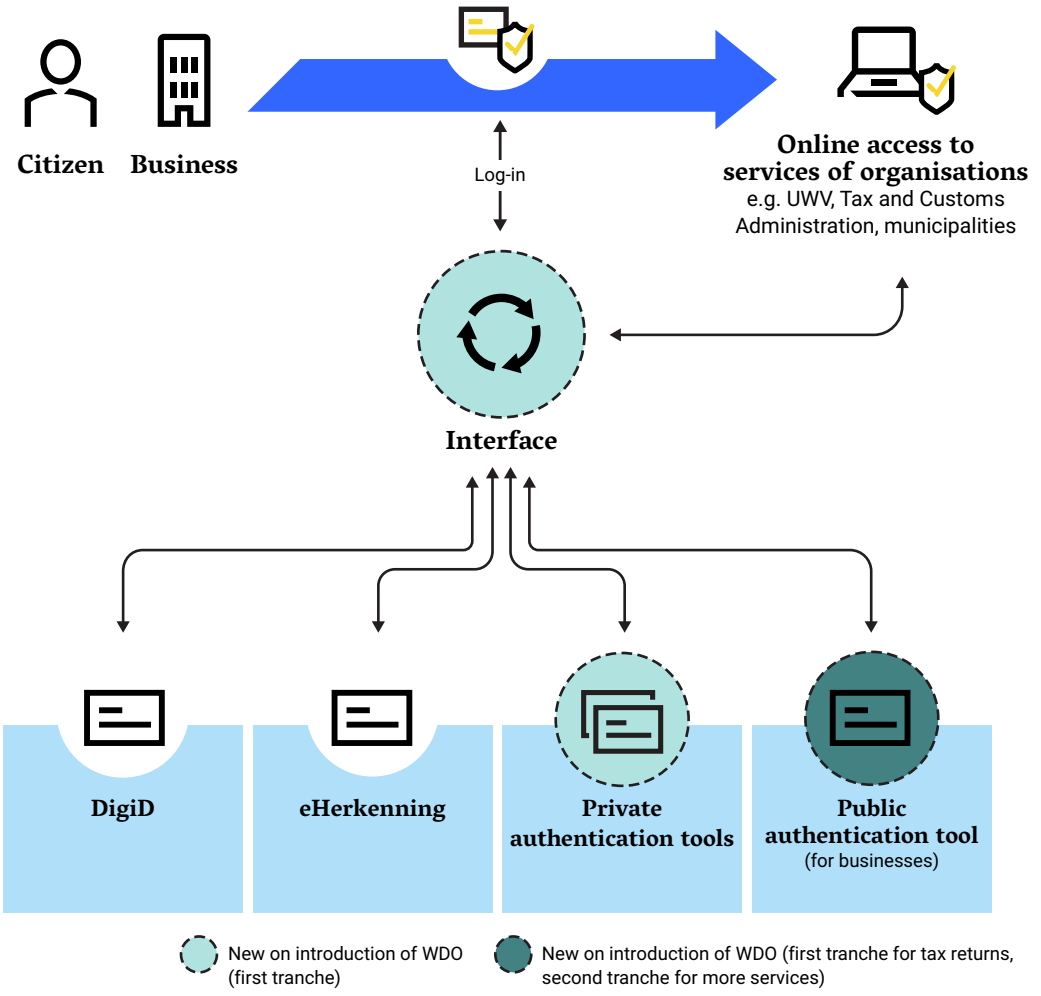


Figure 3 shows that the WDO will allow the admission of private authentication tools (alongside the public DigiD tool). To be admitted to the system, an authentication tool must satisfy the requirements of the WDO. Public parties will be obliged to accept the private authentication tools that are admitted. They must also classify their services by assurance level.

The act will not come into full force on 1 July 2023 but will be phased in. In consultation with Logius, ministries and public service providers, the Ministry of BZK has proposed

a connection timetable for public implementing organisations. Potential providers of authentication tools are expected to apply for admission as from 1 July 2023. The precise conditions must therefore be known long before that date. On completion of this report (February 2023), the conditions were not known.

The WDO also enables implementing organisations to set up a routing facility under the Minister of BZK's responsibility. The routing facility will connect all authentication tools and will thus be an important component of the new authentication system. It is shown in figure 3 as the "interface". At the time of writing, this central interface had not been realised.[16]

The Minister of BZK also wishes to admit a public authentication tool for businesses. In the first instance, it will enable the filing of tax returns. This will be permitted under the WDO bill that has already been passed and will be phased in as from 1 July 2023. The Minister of BZK is still working on a second WDO bill. It is not known when this bill will come into force. In the second part of the WDO, the minister will provide for a public authentication tool for businesses that enables more than the filing of tax returns. After the two parts come into force – the minister refers to them as tranches – the system will look like the one shown in figure 3.

5.3 European digital identity and wallet, eIDAS2

5.3.1 eIDAS2

The European Parliament adopted the eIDAS regulation in 2014. It came into force in September 2018. eIDAS stands for Electronic Identities And Trust Services. It provides a framework for the use of electronic identities and services in the EU. EU member states have agreed to use the same terminology, assurance levels and underlying digital infrastructure for eIDAS.

Via eIDAS, national tools such as DigiD can arrange the same transactions in other EU member states. This means that a Dutch citizen in Germany should be able to arrange the same transactions as a German citizen in Germany.

The eIDAS regulation was not an instant success. Implementation in the member states was less than perfect and too few member states registered their electronic identification tools for connection to the eIDAS infrastructure. As not enough service providers were connected to eIDAS, few services were available. Following an evaluation of the eIDAS regulation, the European Commission itself concluded that it was not satisfactory in all respects (European Commission, 2021).

The European Commission therefore submitted a proposal to the Council of the European Union and the European Parliament to amend the eIDAS regulation with a view to strengthening its operation: eIDAS2 (European Commission, 2021). eIDAS2 also fleshes out a framework for a digital European identity. According to the European Commission, it will strengthen the digital autonomy of European citizens. eIDAS2 must enable citizens and businesses to arrange their digital affairs more simply and securely. eIDAS2 is also a response to developments in the market and the technology available for wallets.

5.3.2 Wallets

In brief, the wallet is a digital folder containing personal information and documentation, such as a driving licence, name and address, certificates and medical information. In principle, only information that is really necessary is shared with another party, either a public authority or a business. You will no longer need to present a passport to buy alcohol, for instance, just show that you are older than 18. Citizens can decide how much they wish to share about themselves with parties requesting information.

The European Commission believes the wallet offers new opportunities for convenience, data minimisation, reliability, security and efficiency. Every EU citizen entitled to a national identity card will be entitled to a digital identity and the associated wallet when eIDAS2 is introduced.

Every member state must offer at least 1 wallet “free of charge”[17] to its citizens. At the very least, the wallet must contain the holder’s identity[18] and an authentication mechanism so that holders can identify themselves online. The wallet will therefore compete against other authentication tools permitted under the WDO, such as DigiD and eHerkenning. We consider this further in the following section.

Wallets will have to be recognised nationally by the designated authorities. The designated authority in the Netherlands is the Dutch Authority for Digital Infrastructure (RDI). A wallet that is recognised in one member state must be accepted in all the other member states. Citizens and businesses can then share their data with other citizens, businesses and organisations. The wallet will be used in both the public and the private domain.

Wallets will also offer functionalities such as an electronic signature. This functionality is currently not offered by DigiD and eHerkenning, see also § 4.2.2.

5.3.3 DigiD and eHerkenning and eIDAS2

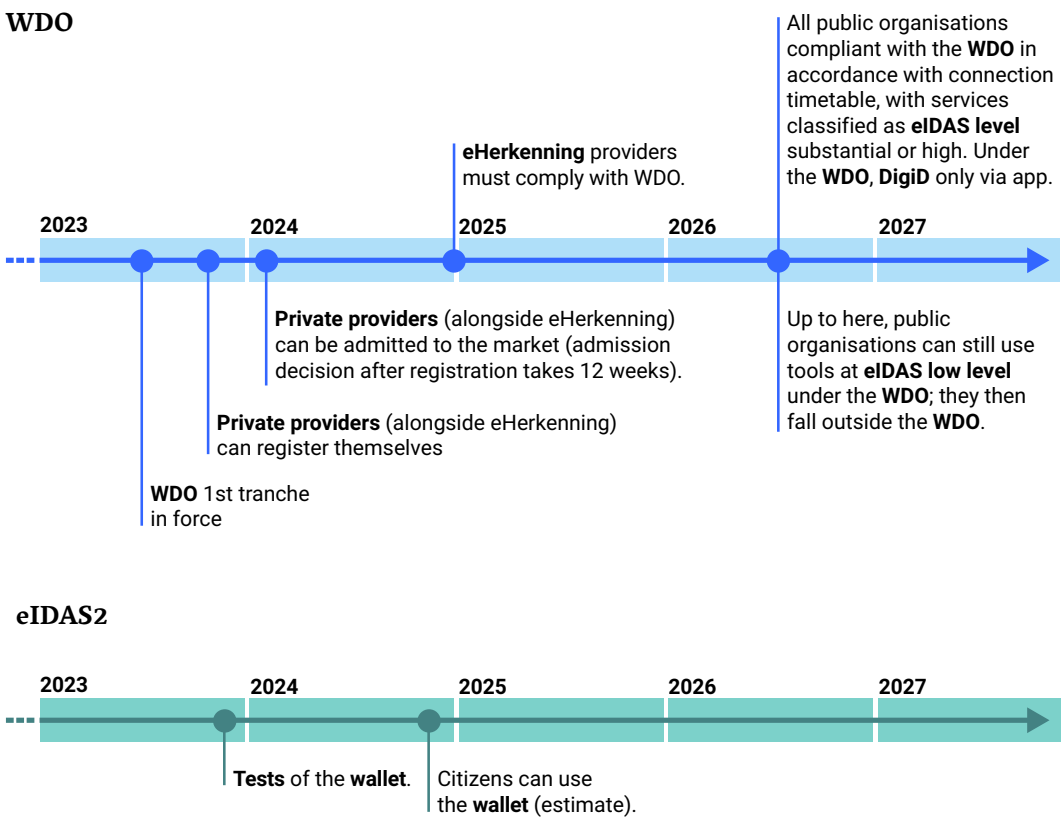
Use of the wallet is voluntary. How quickly it becomes commonplace cannot be said. DigiD and eHerkenning are not expected to become redundant in the next few years. They might not be necessary in the distant future as wallets offer identification and authentication functionalities and allow citizens to manage their own data.

Theoretically, DigiD and eHerkenning can transform into a wallet under their current names but this is not the Dutch government's preferred option. At the end of 2022, the State Secretary for Kingdom Relations and Digitalisation announced that DigiD would not be expanded to become the national pubic wallet but would continue in its current form. The government, however, is studying how a Dutch ID wallet can be activated by means of DigiD. It has also suggested that DigiD could be used as a cross-border eID tool for online transactions with public service providers in other member states (BZK, 2022b).

5.4 WDO and eIDAS2 timeline

Introduction of the WDO, eIDAS2 and the wallet will partially coincide and overlap. Figure 4 shows the indicative milestones.

Figure 4 *WDO and eIDAS2 indicative timeline*



In addition to the milestones shown in figure 4:

- the WDO does not name a date on which the central interface must be available to implementing organisations (as described in § 5.2);
- a timetable will be drawn up in 2023 for implementing organisations such as the UWV, Tax and Customs Administration and municipalities to connect to the new authentication system. Connections must be made within 3 years of the WDO coming into force.

For both of these points, it is uncertain what will happen if citizens try to log in with a new authentication tool in a year's time. If, for instance, a citizen already has a new authentication tool in early 2024 but a municipality does not connect to the WDO system until the end of June 2026, it will take more than 2 years before the citizen can use the new authentication tool with that municipality.

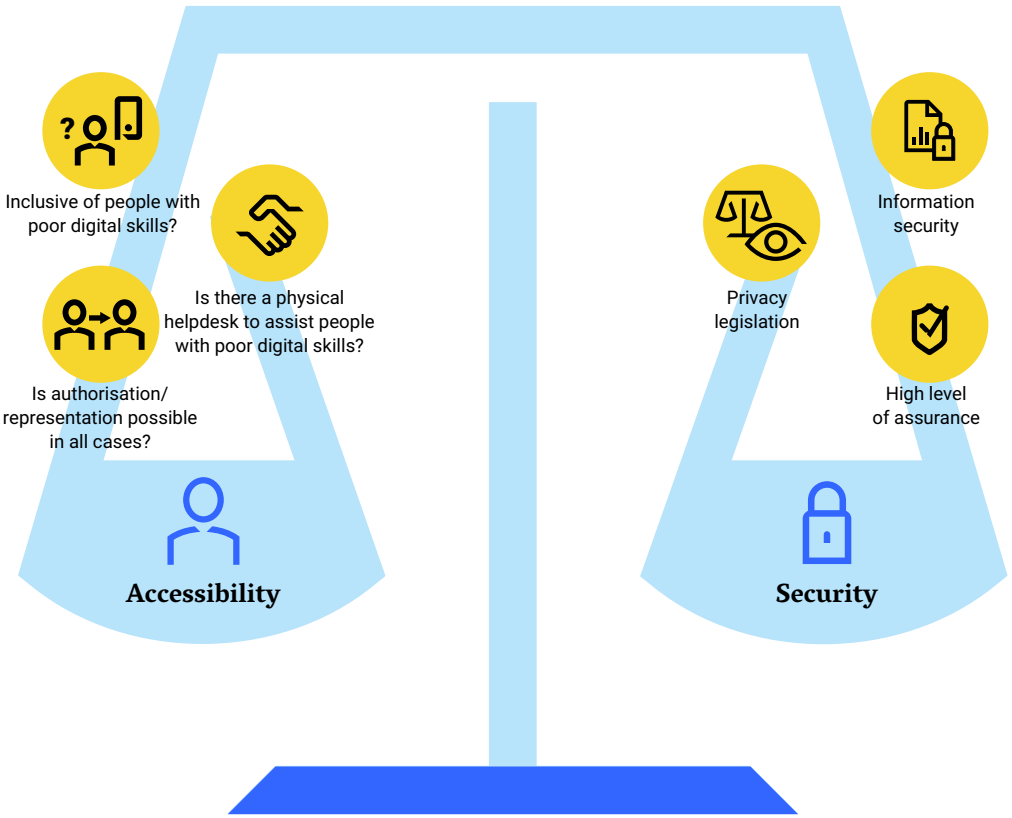
The timeline also has the following risks:

- changes in the system can compromise the continuity and quality of existing services. It is uncertain whether current providers of authentication tools will have enough time to implement the changes (before January 2025) or whether implementing organisations will have enough time to connect to the system (before July 2026);
- staff at the Ministry of BZK and Logius must consider both the continuity of the current DigiD and eHerkenning services and the implementation of the WDO and eIDAS and the wallet. Many activities will be carried out in parallel and will require input from the same scarce expertise and capacity;
- as noted in § 4.4.1, there is little insight into the total architecture of the access system, i.e. the mutual dependence of all components necessary for the system. Shared insight and oversight are needed to design and operate the new system effectively and avoid unnecessary costs.

6. Security versus accessibility

This chapter considers the security and accessibility of the services. Stricter security requirements reduce accessibility. This can create problems especially for people with poor digital skills. The problems can be mitigated if effective assistance is provided, for instance by authorising someone to attend to a person's digital interests or by permitting legal representation. The problems faced by people with poor digital skills can also be mitigated by a physical helpdesk that people with good digital skills can also use if they have a problem that is too complex to settle digitally. Figure 5 shows the considerations at play.

Figure 5 *Considerations regarding the assurance level of DigiD*



6.1 Conclusions

The Minister of BZK decides how secure and accessible digital tools must be. The following points must be taken into account:

- public authorities and implementing organisations increase security by applying higher assurance levels. Increased security is at the cost of accessibility. People with poor digital skills may be excluded;
- this risk can be mitigated by assisting those with poor digital skills.
  - People with poor digital skills can authorise someone to log in on their behalf. This is already possible via DigiD Authorisation. Legal representatives should also be able to log in on behalf of people with poor digital skills but this is not yet possible.
  - A physical helpdesk can assist people with poor digital skills. The Minister of BZK is already funding Digital Government Information Points (IDOs). We found that the limited competences and powers of the IDOs' staff prevented them

from providing effective assistance. A physical helpdesk is also needed for citizens with good digital skills but who have problems that are too complex to settle digitally.

6.2 Security and accessibility

6.2.1 DigiD assurance levels

DigiD has several assurance levels. A higher assurance level provides greater certainty that the person trying to log in is actually who they claim to be. The more factors that are needed to log in, the higher the assurance level. 1 factor, for instance, could be “something you know”, such as a username and password. A second factor could be “something you have”, such as an app on a mobile phone. The assurance level increases further if a physical identification document is checked by means of a built-in identity chip. Implementing parties such as the UWV and municipalities decide for themselves what assurance level is necessary to access their services. The classification of assurance levels in the Netherlands is not the same as the EU/eIDAS classification.

Figure 6 *DigiD assurance levels*

DigiD classification of assurance levels

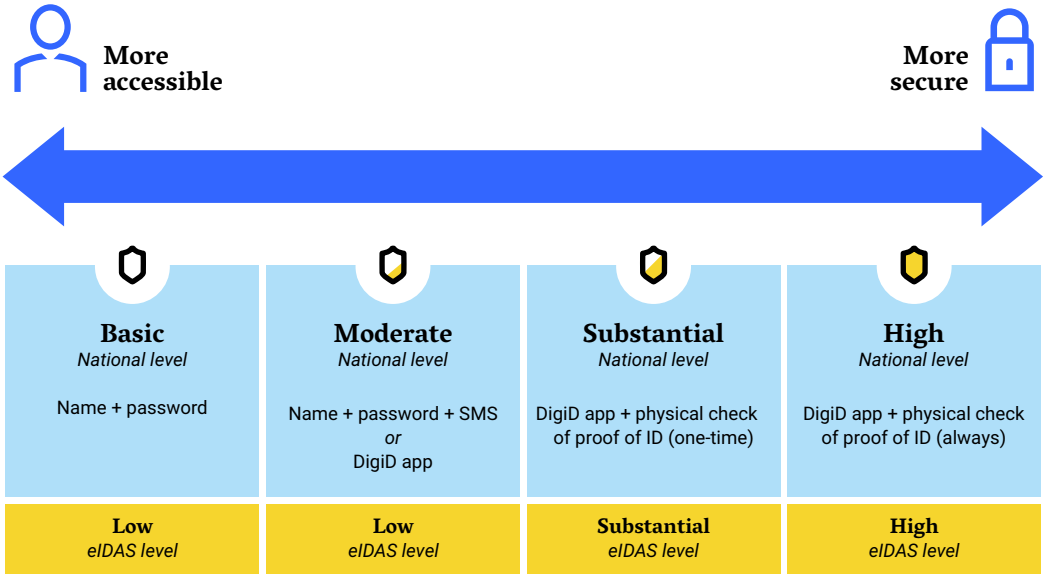


Table 7 shows the number of authentications made via DigiD between 2018 and 2021. The total number of authentications increased during this period, as did the number with moderate, substantial and high assurance levels. There was a decline in the number of DigiD authentications with a basic assurance level. Fewer citizens are therefore logging in using only their username and password.

Table 7 *Number of authentications by DigiD assurance level (ICTU, 2022)*[19]

	2018	2019	2020	2021
Total	307,956,118	340,758,404	402,519,872	557,008,812
Basic	260,066,132	223,949,536	161,210,552	121,523,951
Moderate	47,703,384	111,453,266	195,229,103	281,825,661
Substantial	186,601	5,355,566	46,080,130	153,649,114
High	1	36	87	10,086

Table 8 breaks down the moderate authentications. There are two moderate authentication options: via SMS or via the app. There was an increase in both options.

Table 8 *Breakdown of authentications at moderate assurance level, by app and SMS (also spoken) (based on ICTU, 2022)*

	2018	2019	2020	2021
Moderate (total)	47,703,384	111,453,266	195,229,103	281,825,661
Moderate (app)	10,866,602	46,830,118	95,633,971	132,008,570
Moderate (SMS)	36,836,782	64,623,148	99,595,132	149,817,091

6.2.2 Phasing out of assurance levels

Public sector parties are increasingly opting for higher assurance levels. Since 1 October 2022, for instance, *Mijn Belastingdienst* can no longer be accessed using only a username and password. An SMS code is also required. The same is true of *Mijn Overheid* since the beginning of 2023 and of the Social Insurance Bank as from 8 May 2023. The Benefits Office (*Toeslagen*) will follow at a later date. The State Secretary for Kingdom Relations and Digitalisation has said that the ability to log in by means of SMS authentication will be retained for the time being in view of the many people who still use it (BZK, 2022c).

Use of DigiD at eIDAS low level will no longer be possible 3 years after the WDO comes into force.[20] It will therefore not be possible as from 1 July 2026. Only eIDAS substantial and high levels will still be permitted. Under the WDO, logging in via DigiD will be possible only via the app with a one-time physical check. Tables 7 and 8 show that about 150 million of the 557 million authentications were made using SMS. Many citizens will therefore have to switch from SMS to the app.

Whether they actually will is not entirely clear. The Ministry of BZK has said that in practice services can still be provided at the low eIDAS assurance level. These services will then effectively not be subject to the WDO, but the WDO does not specifically prohibit them.

Careful thought should be given to phasing out log-in options. One factor to be taken into account is whether people with poor digital skills can be assisted properly, for instance by means of authorisation and representation and assistance from a physical government helpdesk.

6.3 Authorisation and legal representation

In § 4.2.2 we briefly considered authorisation and legal representation. In this section we look more closely at the two issues. One of the factors in the consideration of security versus accessibility is whether those with poor digital skills can be assisted, for instance by means of authorisation at their own request or legal representation.

6.3.1 Authorisation

DigiD Authorisation was set up on 1 January 2010. It had previously been known as the Common Authorisation and Representation Facility (GMV) (BZK, 2010). DigiD Authorisation enables citizens, at their own request, to authorise another person or a business to access a particular service on their behalf, for instance to file a tax return. In this example, the authorised person can log in to the Tax and Customs Administration via DigiD on someone else's behalf.

Despite the availability of this functionality, people and organisations are still being "authorised" by non-legitimate means. Without using DigiD Authorisation, for instance, family members can share DigiD information with each other and log in to each other's DigiD account. The move towards higher assurance levels will eventually make this impossible. If you have to log in via the app, you must be in possession of the mobile phone associated with the DigiD account concerned. This can lead to problems among certain groups of citizens.

6.3.2 Legal representation

There are situations in which someone is unable or unwilling to authorise another party. In these situations, too, it may be necessary to log in on behalf of someone else. These situations fall under the umbrella of legal representation.

Parent-child relations

Parent-child relations are an example of legal representation. By law, a parent is a child's legal representative until the child is 18. However, a parent is currently not allowed to log in via DigiD on behalf of a child. For many services this is desirable, especially if the child needs medical care.

Maastricht University Medical Centre has been holding a trial since 8 November 2022 in which a parent with a DigiD account can log in to the patient portal without the hospital's intervention. The hospital checks only whether the parent is competent to do so. The parent then gains access to the child's medical file. Whether – and, if so, when – the trial will be extended or rolled out nationally was not known when this report was written (February 2023).

Administrators and guardians

Some adults with a mental disability are not legally competent and so make use of an administrator. Guardians also administer the property of other people. Administrators and guardians cannot log in on behalf of other people at present. This is because the records of administrators and guardians and for whom they are acting have not yet been released. The government is working on this. On 26 September 2022, the State Secretary for Kingdom Relations and Digitalisation informed the House of Representatives that together with the Council for the Judiciary she would release the register of legal representatives. She would also set up a service to issue declarations on someone's competence to act on behalf of another person. The service will be generic and open to all public sector service providers. She plans to have it start operating in 2024 (BZK, 2022d). Until then, declarations of competence cannot be issued.

6.4 Digital Government Information Points

Citizens with questions about online public services, such as DigiD, can receive assistance from Digital Government Information Points (IDOs). At the end of 2022, there were more than 650 IDOs, most housed in libraries. The network is now almost nationwide, with blank spots only in the rural areas.

The IDOs have received relatively few questions given the size of the potential target group: citizens with poor basic digital skills. In total, about 55,000 questions have been recorded (National Library of the Netherlands, 2022).[21] The Ministry of BZK estimates that there are 2.5 million people in the Netherland with poor digital skills and that about 4 million people do not have the necessary digital and bureaucratic skills to settle their affairs with the government independently (BZK, 2021d).[22]

Table 9 shows that about 20% of the questions received related directly to DigiD.

Table 9 *Types of question received by Digital Government Information Points, 2021 to Q3 2022 (National Library of the Netherlands, 2022)*[23]

Types of question received by Digital Government Information Points	
Other	34%
DigiD: app installation, DigiD application, activation or signing-in assistance	20%
Corona questions (corona check app, vaccination appointments/tests)	16%
Help with computers/tablets/smartphones	14%
Help applying for municipal schemes (e.g. social assistance, social support)	10%
Tax affairs	10%
Manifest Group of implementing organisations (excluding Tax and Customs Administration and DigiD)	4%
Online banking	3%

IDO staff may not apply for a DigiD account on behalf of clients. Under the law, you can only apply for a DigiD account for yourself, not for others. The staff can "look over their clients' shoulders" and help them make the application (Probiblio, n.d.). We found that IDO staff could help people with poor digital skills to only a limited extent because of their limited competences and powers. We recommend that the Minister of BZK determine whether granting IDO staff more powers to help citizens activate and use DigiD accounts would facilitate the further development of IDOs.

We report in more detail on IDOs in our report, Results of the Accountability Audit on the Ministry of the Interior and Kingdom Affairs 2022, forthcoming on 17 May 2023.

Citizens with good digital skills also need a physical helpdesk if they have complex questions that cannot be answered digitally, such as incorrect entries in fraud registers, gender transition issues, immigration and emigration problems and the like. Besides IDOs, municipal helpdesks could also be suitable places to answer such questions.

7. Response and afterword

We received a response to our draft report from the State Secretary for Kingdom Relations and Digitalisation on behalf of herself and the Minister of BZK on 10 March 2023. Her response is presented in full below, followed by our afterword.

7.1 Response of the State Secretary for Kingdom Relations and Digitalisation

“On behalf of the Minister of the Interior and myself, I am writing in response to the findings presented in your audit report *Digital Identity Demanding a Lot from DigiD and eHerkenning*.

Policy objectives for DigiD and eHerkenning

You recently audited the digital authentication tools DigiD (for citizens) and eHerkenning (for businesses). First of all, you note in the report that the policy objectives for DigiD and eHerkenning have been achieved. You further find that the benefits of the tools weigh up against their costs and that the quality of DigiD and eHerkenning is adequately managed. I am pleased with your findings. I will take your recommendations into account in the further improvement and development of the authentication tools.

You report that the authorisation and representation goals have been partially met. My ambition, as set out in the Value-Driven Digitalisation Work Agenda, is to have everyone participate in the digital society. In this respect, I am working on making non-digital means of personal representation widely available (for both authorised persons and legal representatives). You further note that fraud management is spread

across several parties. The Digital Government Act (WDO) provides comprehensive grounds to tackle misuse and fraud. Fraud detection and prevention have my full attention.

Inclusion and accessibility

Higher assurance levels make the service more secure and allow more accurate verification of identities, but citizens' access to digital services must always be borne in mind. The balance between security and accessibility is therefore at the centre of the further development of log-in tools and studies on the application of higher assurance levels.

It can be difficult for citizens to participate in the digital society in full. There must always be physical alternatives in order to contact public service providers. Assistance can be provided by the Digital Government Information Points (IDOs) and DigiD and eHerkenning helpdesks. As noted above, I am also working on the further development of digital representation.

Assisting citizens must come first; IDOs are an important instrument for this. They have been set up for citizens who temporarily cannot help themselves. They provide assistance on access to public services, especially through their "guidance function". I am currently working on the transformation of IDOs into public service Information Points. The role and tasks of the IDO staff will obviously be taken in to account, also with regard to the DigiD application process. I will consider this further in my response to your forthcoming report on IDOs. The One Government project is being developed for digitally-skilled citizens. It is a government-wide national facility to provide information on public services.

The new Access system and the wallet

You state that implementation of the Access system will inevitably require changes in DigiD and eHerkenning. In your opinion, there is uncertainty about the wallet's position in the digital authentication system. I would note that a distinction should be made between the Access system and the wallet, as noted in the proposal to revise the eIDAS regulation.

The proposed wallet will enable more than just authentication. Citizens and businesses can decide what data they keep on themselves, what they are willing to share and with whom. In my opinion, use of the wallet must always be voluntary. Citizens and businesses must not be obliged to use the wallet to authenticate themselves for a public service.

The Access system is a system of authentication tools. In the new system, DigiD and eHerkenning, just like new tools, will have to meet the statutory requirements laid down in the WDO. We are also working hard on conditional access services. You note that there is no central connection point. Instead of a central connection point, a standard interface is being developed. Standardisation will allow service providers to choose their own connection method.

Public service providers should connect to the new Access system gradually rather than all at once. They will gradually connect to the new Access system after the WDO comes into force. The WDO, which provides the grounds for this, is expected to be phased in as from 1 July."

7.2 Afterword

We conclude that DigiD and eHerkenning currently function adequately. The state secretary writes in her response that she will take the content of our report into account in the further improvement and development of the authentication tools. We will follow the state secretary's response to the challenges that will arise in the near future with interest.

We would note that the ambition of having digital legal representatives was first voiced in 2013. We are not aware of a concrete scheme for the national rollout of digital legal representation. Until it is possible, certain groups of citizens will have less digital access to the government.

The state secretary writes that a distinction should be made between the access system (under the WDO) and the wallet (eIDAS2). The relationship between the wallet and the current and new WDO authentication tools and whether the requirements of the WDO will also apply to the wallet are not clear to us.

Implementing organisations must be able to connect to the new authentication tools allowed under the WDO. This underlines the importance of the interface referred to in the report.

Appendices

Appendix 1 Audit methodology

This appendix explains our audit method and activities.

Problem definition

Our key question was:

"To what extent have the digital identity goals and the goals set for the associated authentication tools, DigiD and eHerkenning, been achieved? Are the authentication tools efficient and are their availability, integrity and confidentiality managed appropriately?"

Audit questions

We carried out the audit on the basis of the following questions:

1. To what extent have the digital identity goals and the goals for the current DigiD and eHerkenning services been achieved?
2. How efficient are eHerkenning and DigiD in comparison with each other and with other authentication tools or comparable services at home and abroad?
3. To what extent does the government manage the quality of DigiD and eHerkenning?

We also considered DigiD and eHerkenning in the light of the WDO and eIDAS2.

Approach, assessment and standards

The approach, assessment and standards differed for each audit question.

Audit question 1

To answer audit question 1, we investigated the achievement of the goals set by the Minister of BZK in the past 10 years. We investigated the usage/adoption, functionality and security goals formulated by the minister in parliamentary papers and international declarations. Some goals had not been formulated specifically enough to be assessed. We defined these goals more precisely by means of the assessment framework presented in appendix 2.

To determine whether the goals had been achieved, we collected documentation and held interviews. We then assessed whether the minister had achieved the goals in full, in part or not at all.

Audit question 2

To answer audit question 2, we analysed the costs of the DigiD and eHerkenning authentication tools in the years 2018 to 2021. We also analysed the potential benefits. To compare DigiD and eHerkenning with a foreign authentication tool, we circulated a questionnaire to supreme audit institutions in Europe. We received 12 replies to the questionnaire from 25 countries. Only 1 country had data on the past 4 years and an authentication tool that was somewhat comparable to DigiD.

Audit question 3

To answer audit question 3, we looked at the quality management of DigiD and eHerkenning. We understand quality to mean the availability, integrity and confidentiality of DigiD and eHerkenning. These terms are defined in the glossary.

For audit question 3, we prepared and applied an assessment framework. The framework drew on several sources, such as the Government Information Security Baseline (BIO – and thus international standards ISO 27001 and ISO 27002), the Dutch Government Reference Architecture (NORA) and the eHerkenning assurance system. Several laws and regulations were also relevant, including the Digital Government Act (WDO), the Network and Information Systems Security Act (WBNI) and various EU regulations, such as the eIDAS regulation.

The assessment framework is consistent with certain sections of the Government Information Technology Contracting (GITC) framework of the Central Government Audit Service (ADR), the Handbook on IT Audit for Supreme Audit Institutions and the General Management of IT Services Study Report issued by NOREA, the professional organisation of IT auditors.

We also used the framework to assess activities necessary for the DigiD and eHerkenning services that had been outsourced. Responsibility for these activities cannot be outsourced but the suppliers to whom the activities are outsourced must provide sufficient assurance.

The Court of Audit does not issue a statement of assurance in accordance with NOREA's standard letter for assurance engagements. To answer audit question 3, we carried out an IT audit based on NOREA's quality guidelines We assessed DigiD and eHerkenning against the standards in the assessment framework for. We wanted to know whether, for instance, IT management processes and procedures had been worked out and applied in practice. In audit terms, we assessed the standards based on *design* and *implementation.* We assessed the effectiveness of controls based on the documents provided, interviews and observations made during the interviews we held.

DigiD and eHerkenning in the light of the WDO and eIDAS2

We also considered DigiD and eHerkenning in the light of the WDO and eIDAS2. To do so, we analysed legal texts and documents and held interviews.

Activities

The audit questions were answered by studying a wide range of documents. We studied public sources such as reports issued by audit offices, letters to parliament and documents issued by the European Commission. We also analysed internal sources at the Ministry of BZK and, especially, Logius.

In addition, we held interviews with a wide range of stakeholders. We spoke to staff at the Ministry of BZK, Logius, ICTU (government ICT service), the National Office for Identity Data (RvIG), the Telecommunications Agency and other parties. Appendix 3 includes a list of organisations at which we held interviews and/or that provided information.

We also organised an interactive workshop with representatives from the parties involved in the field. We used the workshop results to further refine the assessment framework and define the scope more sharply.

We produced a series of visualisations, in part to understand the architecture.

Appendix 2 Goals of the assessment framework

The table below describes the digital identity and authentication goals in detail. The Minister of BZK set the goals over the past 10 years. We reference the source documents in which the minister formulated the goals. The sources are listed in the bibliography. The table indicates the extent to which the goals have been achieved and includes an explanation of our assessment.

Table 9 *Assessment framework for the digital identity goals*

No.	Subject	Goal	Goal achieved?	Explanation
B.01a	Usage: scope in the Nether-lands	The systems enable digital interaction with public services and organisations with a public task in the Netherlands (BZK, 2021b).	Achieved	Digital access/interaction/service provision are possible in the Netherlands via DigiD and eHerkenning, with public parties, private parties with a public task and also with private parties (ICTU, 2022). We did not find detailed insight for either DigiD or eHerkenning explaining the extent to which parties must still connect to the systems.
B.01b	Usage: scope in EU	The systems enable digital interaction with public authorities and organisations with a public task in other EU countries (BZK, 2021b, 2021c) (European Commission, 2014) .	Partially achieved	This goal is partially achieved because the number of transactions with other EU countries and the number of services provided are both low.
B.02	Usage: scope (eIDAS)	Since 29 September 2018, Dutch government organisations and private organisations with a public task must allow approved EU log-in tools to access their services (European Commission, 2014).	Partially achieved	Some organisations allow residents of other EU member states to use notified tools and services. However, it is not known which organisations have not yet connected and still have to follow. It is known that not all government organisations accept approved European log-in tools. This goal has therefore been achieved only partially.
B.03	Usage: scope (eIDAS)	European citizens and businesses that have an approved log-in tool must be able to settle the same affairs as all other citizens and businesses in a member state (European commission, 2014).	Cannot be estab-lished	DigiD and eHerkenning are available, notified in Europe, and can also be used in the EU,24 but it cannot be established whether residents of another country can use them to access the same services.
B.04	Usage: scope (eIDAS)	Identification tools have a series of assurance levels reflecting the classification of the data and the nature of the service provided (European Commission, 2014).	Achieved	DigiD and eHerkenning have several assur-ance levels. Service providers themselves are responsible for setting the appropriate level for their services.

No.	Subject	Goal	Goal achieved?	Explanation
B.05	Usage: accessibility	The facilities are user friendly and compatible with mobile devices (without making concessions to security) (European Council, 2017, 2018).	Qualified achievement	In the case of DigiD, key instruments for this are the accessibility requirements/accessibility declarations. DigiD can be used in a browser, where necessary or desired at substantial level in combination with an SMS code (spoken or written) and/or the DigiD app. The DigiD app can also be used on mobile devices. The DigiD app is needed if the assurance level is substantial or higher. The app is available only on Google and Apple platforms. Citizens must register with Google or Apple to use the app. There is no alternative. That is why we make a qualification. Not all eHerkenning providers currently work with apps. eHerkenning providers have made agreements on accessibility, as evidenced by self-declarations.
B.06	Usage: accessibility	The facilities can be used by all users in the same way, including by people with a physical disability, with appropriate assistance where necessary (European Council, 2017, 2018).	Partially achieved	In the case of DigiD, key instruments for this are the accessibility requirements/accessibility declarations. The declarations state that some facilities are not yet “fully accessible”. This is why the goal has been only partially achieved. eHerkenning providers have made agreements on accessibility, as evidenced by self-declarations.
B.07	Functionality	The facilities verify a party’s identity (authentication) (BZK, 2013).	Achieved	With the aid of DigiD and eHerkenning service providers can verify identity.
B.08	Functionality	The facilities support proof of competence for a specific service (authorisation) (BZK, 2013).	Partially achieved	This goal has been achieved for eHerkenning but not entirely for DigiD. Authorisation and representation are still under development.
B.09	Functionality	Everyone can be digitally represented by authorising a legal representative (BZK, 2013).	Qualified achievement	eHerkenning offers this functionality and DigiD Authorisation is available. The qualification is that DigiD does not provide this function for all services but only for individual services.
B.10	Functionality	Everyone can be digitally represented by a legal representative (BZK, 2013).	Partially achieved	This goal has been achieved for eHerkenning. In the case of DigiD, it has not yet been fully achieved for persons under guardianship, under administration and minors. Trials/initial tests are being carried out but completion is not expected for several years. (BZK, 2022d).

No.	Subject	Goal	Goal achieved?	Explanation
B.11	Function-ality	Everyone can digitally confirm a declaration of intent or agree to the substance of a transaction (electronic signature) (BZK, 2013).	Qualified achieve-ment	The functionality is available to citizens and businesses as a trust service, but not as a DigiD or eHerkenning service. The DigiD service does not include a qualified electronic signature. Declarations of intent can be given by means of DigiD or eHerkenning authenti-cation.25 Some eHerkenning parties also provide an electronic signature function.
B.12	Function-ality	The facilities support single sign-on for seamless access to public services (European Council, 2017)	Achieved	Both DigiD and eHerkenning have this functionality, full implementation is not always opportune for security reasons and under applicable laws/regulations.
B.13	Security	Help prevent identity fraud and misuse (BZK, 2013 and 2021c)	Partially achieved	Fraud prevention in DigiD and eHerkenning is spread across several parties, qualitative and quantitative insight is not of the highest order. There is no central fraud notification desk for eHerkenning. The goal has therefore been only partially achieved.

Appendix 3 Organisations interviewed

We interviewed the following parties or received information from them for our audit.

1. ADR (Central Government Audit Service)
2. Telecommunications Agency (AT)
3. Tax and Customs Administration
4. Capgemini
5. Expert Committee for the Supervision of the Electronic Access Services
6. Currence
7. De Waag
8. ICTU (Government ICT Service)
9. Digidentity
10. Itsme (Belgium)
11. KPN
12. Logius
13. Ministry of BZK
14. Ministry of EZK
15. Ministry of VWS
16. National Ombudsman
17. RvIG (National Office for Identity Data)
18. RVO (Netherlands Enterprise Agency)
19. SER (Social and Economic Council)
20. SIDN (Netherlands Internet Domain Registry)
21. Fraud Helpdesk
22. UWV (Employee Insurance Agency)
23. VNG (Association of Netherlands Municipalities)
24. The supreme audit institutions of Belgium, Czechia, Estonia, Finland, Germany, Italy, Latvia, Lithuania, Norway, Slovenia, Spain and Switzerland

Appendix 4 Terms and definitions

Authentication: "*verification of the identity claimed by the entity [..]: is it indeed the entity it claims to be?*" (ICTU, n.d.)

Authorisation: *"determination of whether someone [..] is eligible to access a service or information, etc."* (BZK, 2021c).

Availability: the extent to which an object (information, IT service or IT tool) is continuously available and data processing can continue without interruption.

Confidentiality: the extent to which authorised procedures and restricted powers permit only authorised persons or devices to use an object (IT service or IT tool) or access an object (create, edit, delete or read data).

DigiD: the DigiD name is a contraction of Digital Identity. Citizens can log in to DigiD to access online services from government organisations and other parties.

Digital identity: a collection of reliable data that represent an entity (person, organisation) in the digital domain (BZK, 2021c).

eHerkenning: eHerkenning is a trust framework with a network of public and private parties. eHerkenning authenticates and checks the authorisation of persons wishing to access an online service. This tool is specifically for businesses.

eIDAS: eIDAS stands for *Electronic Identities And Trust Services*. It provides a framework for the use of electronic identities and trust services in Europe.

eIDAS network: the eIDAS network enables people to log in to connected service providers, such as municipalities and the national tax authority, in other European countries using a Dutch authentication tool such as DigiD, and vice versa. A German citizen, for example, can use a German authentication tool to log in to the Dutch Tax and Customs Administration.

Identification: the "*unique determination of an identity in a particular context [and the] answer to the question, which entity is it?*" (ICTU, n.d.).

Integrity: the extent to which an object (data, IT service or IT tool) is consistent with the required reality.

Authorisation: an authorisation service is available for DigiD (DigiD Authorisation). At their own request, citizens can use it to authorise another person to access a particular service on their behalf. An authorised person can log in to the Tax and Customs Administration, for instance, to file a tax return on someone else's behalf.

Wallet: a wallet is a digital folder containing personal information. It can include, for instance, a driving licence, name and address, certificates, medical records, etc. In principle, holders need share only the information that is actually necessary. The information can be shared with public authorities and businesses.

Legal representation: there are situations in which authorisation is neither possible nor desirable, but it may still be necessary to log in on someone else's behalf. Such situations can be resolved by means of legal representation. Legal representation occurs in, for instance, parent-child relations and among adults who are not legally competent and whose affairs are looked after by an administrator or guardian.

WDO: the Digital Government Act (WDO) lays the foundations for the further digitalisation of the public sector. It seeks the maximum possible use of standards and regulates how citizens and businesses access public services digitally. The WDO allows the admission of private authentication tools (alongside DigiD).
The Minister of BZK also wishes to introduce a public authentication tool for businesses. In the first instance, it will be used to file tax returns. This is provided for in the WDO bill that will come into force on 1 July 2023. The Minister of BZK is still working on a second WDO bill. It is not known when this bill will come into force. The Minister of BZK wants this second part of the WDO to provide for a public authentication tool for businesses with more services than just the filing of tax returns.

Appendix 5 Bibliography

Literature

BZK (2010). Letter from the State Secretary for the Interior and Kingdom Relations. *Modernising the Government*. House of Representatives, session 2009-2010, 29 362, no. 177.

BZK (2013). Letter from the Minister of the Interior and Kingdom Relations and the Minister of Economic Affairs. *Information and Communication Technology (ICT).* House of Representatives, session 2013-2014, 26 643, no. 299.

BZK (2019). *Annual Report and Final Budget Act of the Ministry of the Interior and Kingdom Relations 2018*. The Hague: self-published.

BZK (2020). *Annual Report and Final Budget Act of the Ministry of the Interior and Kingdom Relations 2019*. The Hague: self-published.

BZK (2021a). *Annual Report and Final Budget Act of the Ministry of the Interior and Kingdom Relations 2020*. The Hague: self-published.

BZK (2021b). Letter from the State Secretary for the Interior and Kingdom Relations. House of Representatives, session 2020-2021, 26 643, no. 750.

BZK (2021c). Letter from the State Secretary for the Interior and Kingdom Relations. House of Representatives, session 2020-2021, 26 643, no. 743.

BZK (2021d). Letter from the State Secretary for the Interior and Kingdom Relations. House of Representatives, session 2021-2022, 26643, no. 809.

BZK (2022a). *Annual Report and Final Budget Act of the Ministry of the Interior and Kingdom Relations 2021*. The Hague: self-published.

BZK (2022b). *Answer to questions from the de House of Representatives of the States General concerning the European Digital Identity Progress Report* (26643-902). Appendix to parliamentary paper, reference: 2022-0000604333.

BZK (2022c). Letter from the State Secretary for Kingdom Relations and Digitalisation. *Informing Citizens of the increase in DigiD authentication level for certain clients*. Reference: 2022-0000585495.

BZK (2022d). Letter from the State Secretary for Kingdom Relations and Digitalisation. *Access Domain Progress Report 2022*. House of Representatives, session 2022-2023, 26 643, no. 914.

Ecorys (2016). Log-in *Business Case in the BSN domain. The costs and benefits of the eID system*. Rotterdam: self-published.

Ecorys (2018). *Social Cost Benefit Analysis of the Authorisation System*. Rotterdam: self-published.

Ecorys (2023*). Draft Review SCBA Digital Access: In response to the Digital Government Act.* Rotterdam: self-published.

European Commission (2014). *Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*.
European Commission (2021). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) no 910.2014 as regards establishing a framework for a European identity.* COM(2021) 281 final, 2021/0136(COD).

European Council (2017), *Tallinn Declaration on E-Government*.

European Council (2018), *Berlin Declaration on Digital Society and Value-Based Digital Government*.

ICTU (2022). *Digital Government Monitor 2022.* Appendix to parliamentary paper 26 643, no. 945, House of Representatives, session 2022-2023.

ICTU (n.d.). *NORA: Identification and authentication.* Via website www.noraonline.nl.

National Library of the Netherlands (2022). *Output Registration Tool Q3 2022, September 2022.*

Netherlands Court of Audit (2016). *Tackling functional Illiteracy.* The Hague: self-published. Appendix to parliamentary paper 28760, no. 56, House of Representatives, session 2015-2016.

Probiblio (n.d.). *Working with DigiD in the IDO.* Via website www.probiblio.nl.

Internet sources

Chamber of Commerce
https://kvk.nl/

DigiD
https://www.digid.nl/

DigiD Authorisation
https://machtigen.digid.nl/

Digital Government
https://www.digitaleoverheid.nl/

Dutch Authority for Digital Infrastructure (RDI), formerly the Telecommunications Agency
https://www.rdi.nl/

Dutch central government
https://www.rijksoverheid.nl/

EDI Pleio (community for European Digital Identity organised by BZK)
https://edi.pleio.nl/

eHerkenning
https://eherkenning.nl/

eIDAS regulation 2014
https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32014R0910

Electronic signature
https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/vraag-en-antwoord/wat-is-een-elektronische-handtekening

European Digital Identity
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_nl

ICTU
https://ictu.nl/

Logius
https://logius.nl/

NORA (Netherlands Government Reference Architecture)
http://noraonline.nl

Probiblio.nl
https://www.probiblio.nl/omgaan-met-digid-in-het-ido

Register of accessibility declarations
https://www.toegankelijkheidsverklaring.nl/register

Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (eIDAS2)
https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0281&-from=E

Standardisation Forum
https://www.forumstandaardisatie.nl/

Statistics Netherlands
https://www.cbs.nl/

Trust framework for Electronic Access Services
https://afsprakenstelsel.etoegang.nl/

Trusted List Netherlands, Trust Service Providers (eIDAS Dashboard)
https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/NL

Appendix 6 Endnotes

1. More specifically, this authentication tool will initially be available to file tax returns. This is laid down in the first tranche of the WDO. Under the WDO's second tranche, the authentication tool's use will be widened beyond filing tax returns.
2. The trust framework is publicly available on the internet (Source: *Afsprakenstelsel Elektronische Toegangsdiensten*).
3. The figure is a simplified version of the framework. eHerkenning, like DigiD, has several assurance levels that are not shown in figure 2. eHerkenning's assurance levels currently lie between eH2 and eH4. eH2 is the lowest level, requiring only a username and password; at the highest level, eH4, personal data are verified against physical appearance and by means of an original identity document.
4. By way of comparison, in 2021 the population of the Netherlands was 17.48 million (source: CBS). Dutch nationals resident abroad can also open a DigiD account.
5. By way of comparison, eHerkenning is available to all legal entities entered in the Commercial Register. There were 2,199,387 such entities in 2021 (source: Chamber of Commerce).
6. To the end of 2020, some users with more than one account were counted more than once. As from 2021, the Digital Government Monitor decided to monitor only the unique accounts with the highest activated log-in tool.
7. There are several kinds of electronic signature, including ordinary, advanced and qualified. Only qualified electronic signatures satisfy all legal requirements and are always legally valid and equivalent to a wet signature. Source: Dutch central government (subpage). Parties that offer this functionality include KPN, Clever-base and Digidentity. Source: Trusted List Netherlands, Trust Service Providers (eIDAS Dashboard).
8. There is the Central Identity Theft and Error Reporting Centre (CMI) but it does not receive reports of fraud involving eHerkenning and very few fraud reports involving DigiD.
9. Society incurs "costs", but BZK incurs "expenditure" and Logius refers to "income". In our report, we prefer the term "costs" because, in our opinion, this term is the closest to the perception of citizens and businesses and because it agrees with the terminology of social cost and benefit analyses.
10. DigiD Authorisation is often regarded by government as a separate entity, distinct from DigiD and eHerkenning. From a citizen and business perspective, we consider it to be an essential aspect of digital authentication and report these costs accordingly.
11. These amounts are budgeted costs because the actual costs are not disclosed in Logius's annual report and were not provided to us before the audit deadline.

12. The estimate was based on an approximation of the average fee (excluding VAT) charged by eHerkenning providers to issue an account multiplied by the number of eHerkenning accounts issued.
    The costs incurred by implementing organisations such as the UWV and municipalities to connect to eHerkenning via eHerkenning agents are not known and are not included in the estimate. The costs incurred by implementing organisations to connect to DigiD are also not known.
13. Only Latvia could provide this data on time during the audit period. The Latvian audit institution would have to carry out further analyses to calculate the exact number of unique users. It suggested the tool could possibly reach most of the 1.9 million residents. This is about a tenth of the population of the Netherlands. On the whole, there are too many different variables to enable an international comparison.
14. This reasoning is in line with such studies as *Business Case Log-ins in the BSN-domain*. *The costs and benefits of the eID system*. Ecorys (2016):
    "Earlier studies put the average time spent on a paper service by a member of the public at 25 minutes, whereas a digital service costs just 10 minutes. A digital transaction instead of a paper transaction produces a time saving of 15 minutes. Based on an average citizen's hourly salary of €15, the benefit per transaction is €3.75." Page 43.
    The ultimate source of the hourly fee was the average hourly fee in 2015 as calculated by salarisnet.nl. The source of our hourly fee in 2021 is the average hourly salary, source: CBS (subpage). The 'more than 550 million transactions' is taken from Table 1.
    Citizens also spend time installing DigiD, how many minutes they take cannot be estimated. This line of reasoning also holds if we estimate the time saving for citizens at 5 minutes instead of 15. The time saving for businesses and organisations is not quantified but is potentially significant.
15. References to the WDO in this report refer to the act and secondary decrees and regulations.
16. References to "interface" in the report refer to the routing facility. The consultation version of the Digital Government Decree, containing detailed regulations of the WDO, describes the routing facility as follows: "*As a matter of policy, public service providers wish to connect to the electronic access facility simply and once only. Further to the Digital Government Act, a new facility will therefore be introduced, the routing facility, under the minister's responsibility. The routing facility's purpose is to facilitate public and semi-public service providers when connecting to statutory authentication landscapes (DigiD, eIDAS, etc.). The routing facility offers the customer/service provider a single interface, a single contact point and a single*

invoice. The routing facility provides these by acting as an intermediary that passes on electronic message traffic with the authentication landscape on the one hand to the service provider on the other. Technically the routing facility consists of one or more public and possibly one or more private routing services."

17. We would note that nothing is "free of charge". The wallet will be funded from the general budget, from fees paid by connected service providers or paid for otherwise. Given this fact, it is difficult to see what the business case will be for private parties to offer a wallet.
18. The wallet must also be a legally recognised means of identification.
19. The numbers in the table are consistent with those provided by Logius to ICTU for the Digital Government Monitor. The numbers in the Monitor were not reproduced correctly. We received the correct figures by email from Logius.
20. See the Explanatory Memorandum to the GDI Act, part 13, Transitional Law, page 32 (part of the WDO):
    "This bill provides for the use of approved authentication means in electronic traffic with administrative authorities and designated organisations. Only means at assurance level "substantial" or "high" are eligible to be approved. Administrative authorities and designated organisations may provide access to their electronic services at assurance levels "substantial" or "high" if the user logs in with an approved means They are required from the entry into force of this bill to accept approved means. Unapproved means may not be accepted for electronic services at assurance levels "substantial" or "high". There is no transitional law for this. Means with a lower assurance level than "substantial" or "high", such as DigiD, which is due to be phased out, will not be approved under this bill. By way of transitional period, administrative authorities and designated organisations may accept these means with assurance level "low" for three years after this bill coming into force for services with a low assurance level."
21. Number of questions recorded since the launch of IDOs in 2019 to the third quarter of 2022.
22. The figures of 4 million and 2.5 million people are based on studies published in 2013 and 2016. The figure of 2.5 million is taken from the report, Tackling Functional Illiteracy (2016). The Court of Audit wrote in the report: "Two and a half million people over the age of 16 in the Netherlands have literacy and numeracy difficulties". Digital skills were mentioned a couple of times in the report, but the Court expressed no opinion on the number of people with poor digital skills.
23. The percentages do not add to 100%, as the questions relate to several categories.
24. DigiD and eHerkenning have a high degree of acceptance/usage and have been notified to the EU.
25. Signing income tax returns with DigiD is the best known example of this.

Netherlands Court of Audit

Department of Communication

PO Box 20015

2500 EA The Hague

The Netherlands

Phone +31 70 342 44 00

voorlichting@rekenkamer.nl

www.courtofaudit.nl

Cover photo: ANP, Koen van Weel.

The Hague, March 2023