A guide for government organisations

Assurance levels for digital service provision

Version 4

The Standardisation Forum

The Standardisation Forum

The Standardisation Forum was established to facilitate digital cooperation (interoperability) between government organisations and between government, businesses and citizens. Interoperability ensures that different systems are better aligned and integrated and that data can be exchanged and/or reused.

The Standardisation Forum issues advice on research to the National Commission for Digital Government (Digi-commissioner), who in turn makes recommendations to the Digital Government Ministerial Committee on the policies relating to interoperability and open standards. The Forum was established on the initiative of the ministry of Economic Affairs. The Standardisation Forum's secretariat is part of Logius, the digital government service of the ministry of the Interior and Kingdom Relations.

For more information, go to **www.forumstandaardisatie.nl/content/english**.

Foreword

The theme of the governmental Dutch Digi-programme 2016-2017 is 'Human-centred'. As Digi-commissioner[1], I have noticed that it is not always easy to prioritise this theme when choices have to be made in practical situations. Citizens and businesses benefit from a uniform, identifiable government that offers safe and reliable services without unnecessary costs and administrative burdens. As such, a government that makes identical choices in similar cases. As there are so many different public authorities and government organisations, it is not self-explanatory that these choices in similar cases lead to identical service provision.

This Guide to Assurance Levels assists government organisations in making correct choices regarding service digitalisation. The guide pairs service properties with standardised European assurance levels and takes into account i.e. authorisations, information return flows and machine-to-machine message exchanges. It is more or less a toolkit for government service providers, which simplifies how matters such as Single Sign On across government organisations, cross-border services, electronic signatures, stamps and time-stamps are arranged.

The standardisation, made possible by the Guide, renders the government more transparent and uniform. Human-centred! In addition, the government organisations are supported in their digitalisation processes and no longer have to draft individual (risk) assessments to determine which assurance level applies to their service provision. That's efficient!

Providers of authentication devices should categorise their offering in a similar manner as soon as possible, so that government service providers supplying digital services are easily able to make the connection between their needs and the available resources.

I sincerely recommend this new Assurance levels Guide for your perusal. In order to facilitate the adoption of the guide, I will ensure that this Guide – via the management boards and the National Commission – is distributed across the public sector.

Bas Eenhoorn
Digi-commissioner

[1] Bas Eenhoorn (1946) is the National Commissioner for Digital Government (Digi-commissioner). He was appointed by the Dutch Parliament in August 2014. The Digi-commissioners task is to develop a Generic Digital Infrastructure (GDI) that has a high level of operational excellence. The GDI provides government bodies with the basic digital platform to help them organise their primary processes. Thanks to the common use of the GDI, people experience coherence in the government's services, and a uniform way of communication.

MADE IN ENGLAND

List of contents

Appendixes

1 Introduction

What is the reason for this guide?

1.1 E-government: carefully selecting the assurance level

All government services digitalised

The government is committed on a large scale to digital service provision for citizens and businesses. The aim is that all government services are digitally available in 2017. Thus, the objective is to achieve a reduction in administrative burdens, better service provision and a more efficient government.

Obligations for government organisations

This objective creates for you, the government organisation, certain obligations. The Dutch General Administrative Law Act (Awb) applies to you. This requires that electronic traffic between citizens and administrative bodies takes place in a 'sufficiently reliable and confidential' manner. In addition, the Civil Service Data Security Regulations (VIR) states that the governments must determine the assurance requirements for digital services according to a risk assessment, and must ensure that appropriate measures are taken to meet these assurance requirements.
The requirements of those measures have not been specifically defined in the AwB and the VIR decree. For this reason, the State and other authorities have determined so-called standards: the State has the BIR (State Baseline Information Security), provinces have the IBI (Interprovincial Baseline Information Security) and local authorities have the BIG (Municipal Baseline Information Security).

Making choices regarding assurance levels

As mentioned, the requirements are not specifically defined in the Awb and the VIR Decree. However, the increased use of e-services has created the need for clarity. For instance, it is important that government organisations in similar situations require (and ensure) identical levels of assurance for their digital services. It is also vital that their choices are concise and transparent. This contributes to a transparent, accessible, credible and carefully operating government and to the legal certainty of citizens and businesses.

Guide based on eIDAS

This guide assists you in making concise and transparent choices regarding the assurance level of your digital service. We do this on the basis of the eIDAS regulation for digital identification and trust services, which took effect on 1 July 2016. We also include the relevant implementation decrees and the national legislation.

1.2 ‘One size fits all’ does not exist

High or low level not applicable

There are many different digital government services. It is not possible to establish one uniform solution that covers identification, authentication and authorisation for all those services. For instance, in many cases, a standard solution with a very high assurance level is too expensive or simply not required. What’s more, it limits the use of e-services. On the other hand, a standard solution with a low assurance level is not useful either, as it may involve considerable safety risks.

Generic solutions

Citizens and businesses will come across different assurance levels for different services. To prevent users having to manage a large, unwieldy, digital ‘key chain’, the government is working on generic solutions. Examples of this are DigiD, PKIoverheid, eHerkenning and Idensys). Although users are undoubtedly confronted with a choice of level for authentication resource(s), it would ensure that a digital key chain is avoided.

1.3 Use this guide to draft a risk analysis

This guide helps to make choices

Which assurance level should be used in which situation? This is not an easy question to answer for you as implementer of public services. For this reason, this guide was created. It helps you to make a uniform, efficient and informed choice for the assurance levels of digital government services.

Simplified risk analysis with a classification model

This guide contains a ‘classification model’. It allows you to draft a simplified risk analysis of your digital service. The classification model creates a general connection between (types of) services and assurance levels, based on various (legal) criteria. This guide also indicates if a higher or lower assurance level could be required. The guide does not refer to specific authentication methods.

Making informed choices

The classification model can be used by architects, information security specialists, legal experts and directors to help make a reasoned choice for the correct assurance level for your e-services.

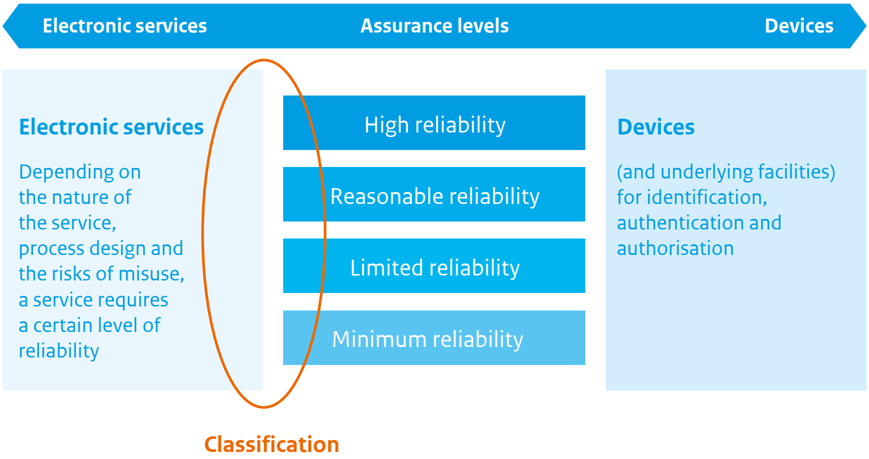
Risk analysis not suitable for every service

Please note: this guide maintains a generic approach. In most cases, this will lead to an adequate choice, but exceptions are possible. It may be that the nature of your service or its circumstances deviate from the classification model to an extent that necessitates a full risk and impact analysis.

Document your selection in a regulation

It should also be added that it is advisable to document the assurance level for your service. This could be policy rules or generally binding regulations, dependent on the context. The accompanying explanatory notes should underpin your choice, so that it is clear for users of the service as well.

Figure 1. *The analysis of the risks in the electronic service determines the required assurance of authentication (in particular) and this in turn determines the strength of the resource used. That is the scope of this guide. eIDAS on the other hand provides a framework for the devices, the assurance provided (see 3.2).*


Electronic services
Assurance levels
Devices
Electronic services
Depending on the nature of the service, process design and the risks of misuse, a service requires a certain level of reliability
High reliability
Reasonable reliability
Limited reliability
Minimum reliability
Devices
(and underlying facilities) for identification, authentication and authorisation
Classification

1.4 How did this guide come about?

Guide since 2011

Various government organisations and businesses worked together on this guide, facilitated by the Standardisation Forum. One of the objectives was to clarify which assurance level was suitable for which (types of) services. This also assigns a clearly defined application scope to standards that outline a specific solution with a specific assurance level.

The Standardisation College has assented to the first version of this guide in the autumn of 2011. The guide was subsequently distributed among government organisations, with advice on how they can anchor the guide in their digital services implementation policy.

Guide under continuous development

The guide is not a static product. Since the first version, the development of e-service provision and identification and authentication devices has been monitored. In addition, experiences with the guide by government organisations are extremely welcome. These are included in subsequent versions. The Standardisation Forum and Logius will continue to support management and further development. This is in line with the management responsibility that Logius assumes for various identification and authentication devices and standards, such as DigiD (authorisation), PKIoverheid and eHerkenning.

Community to keep guide up to date

The parties involved with the first version of the guide form the basis for a 'community' of users. The community helps the Standardisation Forum to maintain and further develop the guide. For instance, in its second and third versions, the guide has been enhanced with topics such as authorisations, one-time login, and electronic authentication and signatures.

Amendments in version 4

The current version 4 focuses on the transition to the e-IDAS regulation. Furthermore, chapter 9 on signatures has been updated to reflect recent developments. The previous normative elements for signature solutions have been deleted. Generic solutions such as eHerkenning and Idensys offer devices for this. The appendices on legislation have also been updated.

Not for private service providers

We deliberated whether version 4 should also be aimed at private providers of digital services. We eventually decided against this, as the legal basis for these providers is essentially different. Does your government organisation also operate under private law? For example, through exploitation of sports accommodations? Then we still recommend this guide. This way, you treat these digital services the same way as you do your private digital services.

1.5 Reading guide

Chapter 2-4: the essence

Chapter 2 describes the demarcation and context of this guide. What is it about and what is it not about? Chapter 3 contains the principles for the elaboration of the classification model. In chapter 4, we go into more detail about our methodology. This is where you will find the actual classification model for rating your services at the required assurance level. These three chapters form the essence of the guide.

Chapter 5-9: specific services

Chapter 5 until 9 deal with specific types of communication or service provision. We will look into: authorisations, application-application traffic, return flows, single sign-on, and signatures.

Appendices: legislation, examples and definitions

Appendix 1 describes the legal framework for classification of services for the required assurance level. Appendix 2 contains examples of the way in which legal requirements and formulations are translated into digital practice. Appendix 3 lists commonly used terms.

2 Demarcation and context

What is this guide about?

The reliability of the government's digital service provision is a large and complex domain. After all, the functions and tasks of the different government departments are essentially diverse. It is impossible to cover this domain in its entirety within just one guide. This chapter explains what we will focus on. This 'demarcation' will also briefly discuss relevant trends and developments. Definitions of terms, such as the 'assurance level', can be found in appendix 3.

2.1 Demarcation

2.1.1 Which services are included?

This guide will discuss in detail the services and processes offered by the government to citizens and businesses. This broadly includes services where:

1. a citizen or business makes use of a service via Internet and also carries out the required actions independently. For instance, a visit to a website that involves a transaction or sending an e-mail;
2. someone carries out the required actions on behalf of another (natural person or legal person) party ('authorisation');
3. automated systems communicate without direct human intervention.

2.1.2 Solely for individual services

This guide helps to determine the required assurance level for one particular service. Of course, you may offer more than one service. This might mean that, in accordance with the risk analysis in this guide, you arrive at various assurance levels. The application of risk-mitigating measures to your service could offer a starting point for reducing the number of assurance levels for your organisation (along the dimension of risk-reducing aspects as listed in chapter 4).

2.2 What are the current trends and developments?

Which current developments and trends are relevant to the assurance level at which services are offered? We distinguish six items, explained in more detail below.

2.2.1 Outsourcing and external trust services

This guide presumes that you offer an individual service that is also designed and managed by you. However, there is a trend where an increasing number of government service providers outsource their digital trust services, in part or in its entirety. In that case, the design or the management of the trust services lies with an external party, for example.

As the service provider, you maintain firm requirements. You should also be able to keep a tight rein on the service provision by this external party.

In outsourcing, you remain responsible for the reliability (availability, integrity and confidentiality) of your service. This means that you must determine the required assurance level of your service. In addition, you must impose strict requirements on the reliability and quality of your external suppliers and their authentication solutions. Also, accountability and monitoring should be arranged properly. It does not matter in principle whether you use a market participant or the government's shared facilities.

Relevance for this guide

We do not comment on how you can safeguard quality and reliability in outsourcing, for this we refer you to VIR, BIR, IBI, BIG and – for instance – the guidelines issued by the National Cyber Security Center (NCSC).

2.2.2 European regulations and NEN standards

Two new European regulations are relevant to assurance levels. First of all, eIDAS. This will be discussed in further detail in chapter 3. There is also the General Data Protection Regulation (GDPR, in Dutch: *Algemene Verordening Gegevensbescherming _ AVG*), which formally comes into force on 25 May 2018. All government service providers have to comply from that date.

General Data Protection Regulation (GDPR)

The GDPR comprises tightened rules for the protection of (special) personal data. Non-compliance could mean high fines. The GDPR differs from the current Dutch privacy legislation in accordance with the Personal Data Protection Act (In Dutch: Wet bescherming persoonsgegevens Wbp).
A list of some important differences:

- The obligations in the GDPR are much more detailed in many aspects. It also describes how you should meet the standard.
- There is a focus on accountability. If you process personal data, you are not just obliged to describe the processing chain, but also design and implement it in a way that allows you to demonstrate you comply with the law.
- As well as adequate security, you must also ensure that you carry out 'privacy impact assessments' and apply 'privacy by design'. All this should be documented.
- You are required to pay a lot more attention to the way in which you inform those involved about processing their personal data. You will also need to implement processes to comply with the rights of access and correction.

NEN[2] standards

In addition, there are the Dutch NEN standards on authentication, referred to in the legislation. These standards are an example of how standards influence the required assurance level in specific sectors. For example, the NEN 7510 relates to the Use of the Citizen Service Service Number in Care Settings Act (Wbsn-z). This standard mentions two-factor authentication[3] for access to a medical information system: 'Information systems that process patient data should apply authentication based on no less than two individual characteristics.'

2.2.3 Governments process increasing volumes of special personal data (with or without professional confidentiality)

The trend is that an increasing volume of special personal data is being processed by (decentralised) governments. Governments also process more data that are protected by professional confidentiality (see box).

Example: decentralisation of care and wellbeing

Various forms of care and wellbeing have been decentralised to municipal services. This means that local authorities are processing more and more health data and other special data. What's more, they increasingly have to deal with information that is subject to medical confidentiality.

Another example is the data processing for Youth Care by local authorities. Youth care providers have a documentation obligation. This is comparable with the documentation obligation in the Medical Treatment Contracts Act (WGBO) for care providers in a treatment setting. They are also subject to professional confidentiality. This is about everything the care provider knows about the patient or documents in the patient file. Local authorities also have to process information regarding access to and settlement of youth care.

Relevance for this guide

This trend is relevant for this guide. It shows that the need for higher assurance levels is increasing.

[2] Dutch Standardization Institute, national partner of CEN, the European Committee for Standardization.

[3] Two-factor authentication means that access is only possible with something you know (a password or code), together with something you have (a pass or token).

2.2.4 Governments increasingly process data digitally

Governments increasingly process data digitally. This includes the interaction with citizens and businesses. Programmes such as Digitaal 2017 reinforce this trend. This trend shows that (almost) all services provided by the government are available in digital form, often still parallel to the 'traditional' forms of service provision (at the counter, in writing). What's more, digital is increasingly becoming the government's preferred medium. It is also expected that more and more, digital will be the only option offered, such as for Income Tax returns and for procurement. The latter will always be considered on an individual basis for each service by the legislator.

Relevance for this guide

The National Ombudsman said in the report 'The disappearance of the blue envelope' (5 April 2016) that 'people who struggle with digitalisation must be able to receive adequate support'.
This in particular demands proper facilities for authorisation by citizens to fellow citizens and organisations, as well as some restraint in making the digital medium mandatory. Facilities for authorisation could include organisations that act as intermediaries. Logius is working on creating a citizens' organisation authorisation in DigiD Authorisations.

2.2.5 Service providers 'within the Citizen Service Number – BSN[4] domain' use trust services from the market

Service providers within the BSN domain are increasingly using authentication devices and trust services from the market. This includes the authentication of citizens and is no longer solely for organisations. For now, this mainly concerns eHerkenning and the tests with iDIN in the BSN domain (login to Tax and Customs Administration with bank card) and Idensys.

The service provider undoubtedly has and will have ultimate accountability for the overall reliability of its service and authentication solution used.

Relevance for this guide

There is no need for revision of this guide's scope in response to the trend. It is a trend that had already been taken into account during the first outline of this guide.

[4] The citizen service number or Burger Service Nummer in Dutch (BSN) is a unique personal number allocated to everyone registered in the Municipal Personal Records Database. Your citizen service number is recorded on your passport, driving licence and identity card.

2.2.6 Mandatory use of authentic data from key registers

Use of authentic data from key registers should be mandatory for all organisations with a public sector remit. If this is the case, the organisation involved no longer requests these data from citizens or businesses. It concerns data from, for example, the Key Register of Persons (*BRP*), the Trade Register (*HR*), the Key Register of Addresses and Buildings (*BAG*), the Cadastral Key Register (*BRK*), the Key register of Vehicles (*BRV*, also Vehicle Registration Register), the Key Register of Income (*BRI*) and the Key Register for Valuation of Immovable Property (*WOZ*). This increases the importance of a sufficiently high assurance level for access to the key registers.

Relevance for this guide

This trend is relevant to the guide, as it means a higher assurance level is required more frequently. In relation to this matter, we distinguish between two situations. First of all: consultation only, in which case the data consulted and the messages sent regarding those data should be very reliable above all. However, the second case is that the key register is used in addition to changes being made to the key register. In that case, it is vital that the user has been authenticated with high assurance.

3 Principles

Simplified risk analysis based on eIDAS

This chapter describes the principles of the guide.
These are:

- The essence of the guide is a simplified, easy to manage risk analysis.
- The guide utilises the eIDAS assurance levels.
- The guide utilises the eIDAS trust services (see chapter 9 and parts of chapter 7).

Thanks to this approach, it is relatively easy to make a global estimate of the risks of your specific service, allowing you to swiftly determine the required assurance level.

3.1 Simplified risk analysis

Various countries use risk analyses to classify assurance levels.[5] The United States have also opted for this approach. For this purpose, the Office of Management and Budget established the EAuthentication Guidance for Federal Agencies[6] in 2006. This contains a detailed risk analysis, due to the culture of accountability in the United States.

Systematically, based on objective criteria

In the Netherlands, such a costly, time-consuming and fragmented approach overshoots the mark. We would prefer to use the characteristics of processes and services as starting points for determining the desired assurance level. This guide has attempted to find a system suitable for generic estimation of risks. We estimated the value to be protected on the basis of several objective (or objectifiable) criteria and interests. This included statutory requirements, the nature of the data exchanged (personal data or not) and the economic or societal significance of a service. Then, we estimate the possible damage in case incorrect authentication was to take place.

[5] See example from Spain: MAGERIT, Methodology for Information System Risk Analysis and Management; Ministerio de Administraciones Públicas, June 2006, *http://rminv.enisa.europa.eu/methods/m_magerit.html*

[6] *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800632.pdf*

Assumptions about (IT) security

We also presumed that the relevant services were provided from similar online environments and display similar vulnerabilities. To prevent these vulnerabilities, the DigiD[7] ICT Security Assessment Standard is applicable, as well as the guidelines from the National Cyber Security Centre (NCSC) on which these are based[8]. In addition, we presumed that the services implement at least the Standard for DigiD.

We also took into account the fact that 'offline' measures can also be taken to ensure the reliability of data and to reduce the chance of interchanged or falsified identities.This could include feedback via a letter to the residential address or actual attendance at a counter.

This risk analysis for assurance levels can be considered as a specific interpretation of a broader risk analysis for information security. This approach deliberately links in with the regulations for information security in the Netherlands.

Read more about our methodology

Our methodology is presented in chapter 4. Complete this simplified risk analysis in its entirety to determine the assurance level you require. Would you like an initial indication of the correct assurance level? Then take a look at the examples in paragraph 4.4.

New types of services

Digital services are changing all the time. New types of services are on the rise, such as:

- services via an app, like the Student App by DUO or the Income Tax Returns App by the Dutch Tax and Customs Administration;
- continuous data exchange based on specific devices, possibly linked to a type of subscription. This could include smart meters, devices in cars that continuously exchange data, medical applications where users register, monitor and edit measurements on a regular basis.

[7] Version 1.0 dated 21 February 2012 see *www.logius.nl/ondersteuning/digid/beveiligingsassessments/*

[8] Current version is 2.0, whilst the DigiD ICT Security Assessment Standard is still based on version 1.0.

These developments have not led to genuinely new types of government services as yet. The current generation of apps offers comparable services as those offered via websites and portals. However, it is likely that completely new applications will also arise and that this will change the assessment of assurance levels. The use of these applications is currently still limited. Therefore, this development does not yet necessitate changes to this guide.

3.2 eIDAS regulation as a foundation

The European eIDAS regulation came into force on 1 July 2016. eIDAS stipulates criteria for the assurance levels of authentication devices. There are three levels: low, substantial and high[9]. This regulation means there is a legal framework for determining assurance levels for digital government services. This fourth edition of the guide is the first time eIDAS is used as a basis[10]. For further introductory notes on the regulation, see appendix 1.

The three eIDAS levels are explained below. The explanation will assist you in applying this guide.

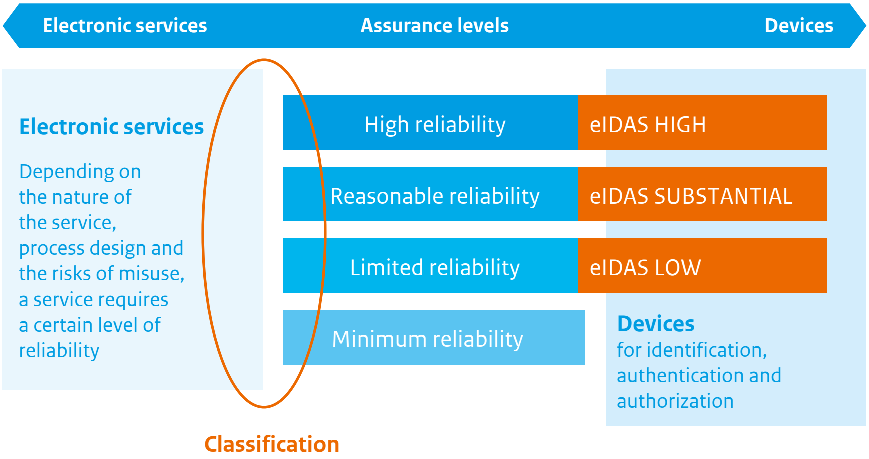
Only for authentication

eIDAS is aimed at the authentication of citizens and businesses, and particularly on web portals. There are hardly any generally accepted standards available for classification into assurance levels when it comes to other activities, such as authorisations and application-application traffic. However, this guide does provide further definition of the above.

[9] Up to version 3 of this guide, there was no legal framework yet. The STORK classification model was used instead.

[10] We also maintain eIDAS for the national assurance level of services, although strictly speaking, eIDAS only regulates cross-border authentication and associated authentication devices.

Figure 2. The guide deals with the classification of electronic services in order to determine the desired assurance level, particularly for authentication.



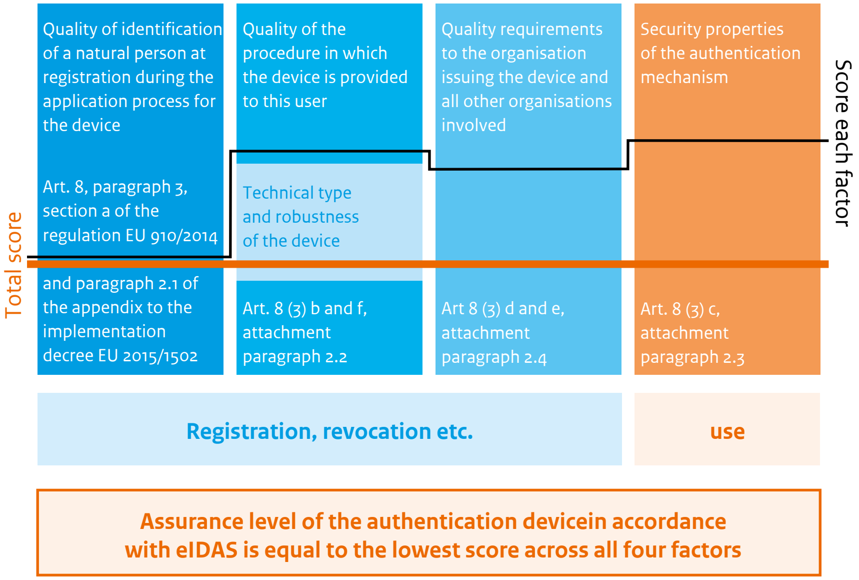
3.3 eIDAS: three assurance levels

In order to determine the assurance level, eIDAS maintains minimum requirements for each level, and poses the following questions:

- How good is the **identity verification** of a person requesting a resource?
- How good is the **procedure** used to issue the device
- to a user?
- What is the quality of the **organisations** involved with issuing the device and the registration?
- What are the **technical specifications** of the authentication device?
- How does the **authentication mechanism** work that is utilised to identify the user of a digital service?

These factors are first assessed separately. Then, the final assurance level of the authentication device is determined through the lowest score for the individual factors. This is depicted in the figure below.

***Figure* 3.** *eIDAS provides four factors for scoring an authentication device. The lowest score determines the final level of the authentication device.*



Quality of identification of a natural person at registration during the application process for the device
Art. 8, paragraph 3, section a of the regulation EU 910/2014 and paragraph 2.1 of the appendix to the implementation decree EU 2015/1502
Quality of the procedure in which the device is provided to this user
Technical type and robustness of the device
Art. 8 (3) b and f, attachment paragraph 2.2
Quality requirements to the organisation issuing the device and all other organisations involved
Art 8 (3) d and e, attachment paragraph 2.4
Security properties of the authentication mechanism
Art. 8 (3) c, attachment paragraph 2.3
Score each factor
Total score
Registration, revocation etc.
use
Assurance level of the authentication devicein accordance with eIDAS is equal to the lowest score across all four factors

Additional requirements

As well as the requirements above, eIDAS also has specific requirements for: the minimum range of personal data that must be used for identification;

- the conditions of use;
- the upgrades to the device;
- the information security;
- (independent) audits;
- accountability.

Level 1: eIDAS low

The first minimum requirement from eIDAS for **identity verification** is that the identity data provided by the user, should be verifiable in a key register. In the Dutch situation, this relates to the Key Register of Persons (BRP). The check in this key register has to be carried out. However, the user does not have to appear in person during the registration process.

A **device** with one-factor authentication will suffice. This could include a combination of a user name and password or a unique code that is sent to the user by a trusted party.

The **objective** of eIDAS is to diminish the risk of misuse or editing of the identity. This is done by establishing that the user is a uniquely identifiable person, someone who has been verified as an existing person by the government. However, a limited amount of trust applies to digital services. It is not entirely certain that the person visiting the electronic service is really the person whose identity you, as provider, are provided with.

DigiD (basic) is an **example** of a device at eIDAS level 'low'.

Lower than eIDAS 'Low'

Many authentication devices do not comply with the requirements for eIDAS 'Low'. They are level 1 devices in accordance with STORK and ISO29015[11]. An example is an e-mail containing a verification link that the user only has to click to start using the authentication device.

Level 2: eIDAS substantial

Stricter methods for **identity verification** are required within eIDAS substantial. When a user requests this resource, it has to be established that he/she is in possession of a valid, official document with the same identity information, which can be checked in a key register. This check [12] can be outsourced or be carried out remotely. The check should offer a substantial level of trust.

The type of **method** required is two-factor authentication. The device should be designed in such a way that it can only be used under the control of the user. It must not be possible that another person is able to use it by accident or unwittingly.

Finally, eIDAS substantial requires a prerequisite for the **authentication mechanism** itself. There should be dynamic authentication: the (cryptographic) data for the authentication should change for each use. This offers extra protection against fraudsters trying to steal and reuse data. An example of this is one-time password tokens.

[11] And has also been described as such in previous versions of the guide.

[12] The exact interpretation of the requirements for this check is undoubtedly still subject to further development and harmonisation between the member states.

Examples of devices at the eIDAS substantial level are the bank tokens (presuming that the identification verification in the registration and issue process was sufficiently reliable).

Level 3: eIDAS high

For eIDAS high, the user has to appear in person at least once in addition to the requirements set for level ‘substantial’.

Furthermore, the **device** must be well-protected against misuse by others. This could include a cryptographic token that also requires a PIN code before use. This PIN code offers extra protection against misuse by third parties.[13]

[13] The requirements are almost as strict as those for devices for qualified electronic signatures. Unlike the previously used STORK, eIDAS high is not equal to the qualified electronic signature nor its associated technology.

4 Classification of services

How do you choose the correct assurance level?

Chapter 3 contains formulations for a classification model for rating e-government services according to the various assurance levels. This chapter explains this model. You could regard it as a simple risk analysis. The choice of assurance level depends on several criteria. These criteria are in relation to:

- the legal requirements of the service;
- the nature of the data and how they are processed;
- the potential damage from misuse of the data.

Table of the classification model

Page **29** shows the criteria in a table for a concise overview. This is the classification model. It allows you to make an initial estimation of the assurance level. Subsequently, read the explanatory notes for the criteria in this chapter for a detailed assessment for each criterion.

Analysis based on one scenario

Our methodology does not estimate the likelihood or impact of a threat. Instead, we use one scenario, the so-called reference scenario. Assumptions are made about, for example, the quality of the IT security and the back-office processes of the service.

Deviation? Carry out a complete analysis

The classification model has several adjustment factors. These are relevant when the threat significantly varies from the reference scenario and is higher or lower, for instance. Did you observe a higher threat level? Then do not just accept this simplified risk analysis, but carry out a complete risk analysis.

4.1 Classification model and criteria

You will come across various criteria in the classification model. These are linked to the assurance levels. Consider which criteria are applicable to your service. Some criteria may show a low score, others a substantial score. The highest score determines the desired assurance level for your entire service.

The following criteria are relevant for rating the assurance level of your service:

1. Are **personal data** processed (see subsection 4.1.1)? If yes:
   - what is the nature of the data that requires protection? Are special personal data processed too? Are data such as the Citizen Service Number (BSN) or medical data processed?
   - what are the relevant characteristics of the processing operation itself?
2. What are the **legal consequences** of the use of your service (see subsection 4.1.2)?
3. Does your service make changes to **key register data** (see subsection 4.1.3)?
4. How substantial is the **economic interest** of your service (see subsection 4.1.4)?
5. How substantial is the **public interest** of your service (see subsection 4.1.5)?

What if a device of the correct assurance level is not commonly available?

It may happen, especially in electronic service provision to citizens, that the relevant target group do not yet have sufficient access to an authentication device with an adequate assurance level. In fact, we are currently talking about the available assurance level for DigiD, in the longer term also about the availability of other authentication devices from private parties allowed in the public domain.

In case the desired assurance level is not yet (adequately) available, the following general rules apply:

- Opt for electronic service provision where you make the next lower assurance level mandatory, that is (adequately) available.
- In this case, also encourage the use of an authentication device of the desired assurance level, in case citizens are able to use it but not yet do so. This way, a target group can move towards the correct assurance level gradually.
- Take compensating measures that make the extra risk acceptable, which follows from the choice for the lower assurance level.

Please find below the table showing how the criteria lead to the choice for an assurance level first. Then, in the paragraphs that follow, we will discuss each criterion separately and in detail. Please note, this concerns indications of an assurance level that is applicable to a standard or reference scenario (see paragraph 4.2) Your specific situation may involve adjustment factors (see paragraph 4.3).

Criteria	Assurance level (according to eIDAS)
• No processing of personal data (class 0) • No Citizen Service Number (BSN) • No legal consequences • No modification to key register • No economic interest • Public interest not applicable	No requirements for authentication
• Personal data maximum class 1 • BSN personally provided or implicitly in authentication • Possible indirect legal consequences • Modification of non-risk key register data only • Minor economic interest • Public interest low	Low
• Personal data maximum class 2 • Aggravating factor for personal data in addition to class 1 (nature of processing) • BSN processed in combination with additional personal data • Direct legal consequences • Provision or modification of key register data that do not fall under 'high' • Moderate economic interest • Moderate public interest	Substantial
• Personal data class 3 • Aggravating factor for personal data in addition to class 2 (nature of processing) • BSN processed in combination with additional personal data • Direct creation, mutation or effectively terminating (authentic) key register data • Significant economic interest • Significant public interest	High

4.1.1 Does your service process personal data?

There are roughly two conceivable scenarios in this guide. Data from businesses or organisations are processed. Or personal data are (also) processed. The latter is often the case.

Personal data requires security

Processing personal data requires a broad range of safety measures. You must be certain that only those authorised have access to the personal data, for instance through authentication 'at the gate'.

Criteria for risk analysis

What is the risk of personal data processing? The main criterion is the **nature of the personal data**. After that, it is the **nature (operation) of processing**. This is also how it is described in the Guidelines for Data Protection from the Data Protection Authority (AP). The guidelines should be conceived of as a further elaboration on the security obligation in article 13 of the Personal Data Protection Act (Wbp).

How can we make the personal data criterion applicable?

In order to tackle the 'nature of personal data' criterion, we divide the personal data into various classes. This classification is inspired by a publication from 2001 by the Data Inspection Board, the forerunner of the AP, on the protection of personal data (hereafter: AV 23). The guidelines by the AP replace AV 23. However, the considerations in the guidelines do include aspects from the AV 23.

New guidelines

For the recent guidelines, a methodology has been chosen that links in with the common practices in information security. They offer you, the responsible party, the flexibility to take security measures that are most suitable for your situation. It makes the guidelines less static than the framework offered by the AV 23. It matters that all circumstances are considered for each case. After all, you should include all of them in your risk weighting.

Consequence for this guide

The AV 23 assigns a certain risk to the nature of data in case of processing of those data. Previous versions of this guide were related to this risk classification. This classification remains relevant in the current guidelines too. Therefore, we do not deviate from the risk classification that is linked to certain types of data in this version of the guide, unless there is a different development or improved understanding. We base this guide on AP research and on recent guidelines.

For the record: the division of personal data into classes is not relevant for the 'nature of processing' criterion (see page **34**).

Obligation: comply with the Personal Data Protection Act

Aside from data types and how you rate these using this guide, article 13 of the Wbp determines the necessity for carrying out a risk analysis for the information security. After all, you have to comply with the Wbp across the board. So, this concerns the total information security, with this guide only offering a (simplified) risk analysis for the authentication (as part of said information security).

Ensure suitable security

The Wpb requires suitable security measures for personal data. But what does 'suitable' mean? The guidelines explain how the AP applies the security standards from the Wpb when investigating and assessing the security of personal data. This way, the guidelines create a link between the legal domain and the information security domain. It is therefore important for suitable security that the guidelines are used together with generally accepted security standards for information security, such the ISO/CIE 27001 and the ISO/CIE 27002.

AP: directions for determining the assurance level In the guidelines

The AP provides practical directions on the correct assurance level for various types of data processing. It is important that you know the risks (of a negative effect on personal privacy) for the person(s) involved in data misuse. Then, you use the awareness of those risks to determine which measures need to be taken: which assurance requirements can prevent those risks? In order to do this, you must be aware of the consequences of all possible types of loss or unlawful processing of personal data. This could include stigmatisation or exclusion, damage to reputation, damage to health or exposure to (identity) fraud and invasion of privacy.

Defining: nature of the data and processing

In order to determine the assurance requirements, the risks for one individual person involved are decisive. The damage he/she experiences due to loss or unlawful processing of his/her personal data depends on the nature of the data and processing. Therefore, ask the following questions for assessing the assurance level:

1. Is there an appropriate security level in view of the risks surrounding **the nature of the data that need to be protected**?
2. Is there an appropriate security level in view of **the risks surrounding (the nature of) processing**?

These questions are discussed in more depth below.

Ad 1: Is there an appropriate security level in view of the risks surrounding the <u>nature of the data that need to be protected</u>?

The AP mentions, among other things, data with a higher and high risk: Special personal data as referred to in Wpb article 16.

1. This includes personal information on someone's religion or beliefs, race, political affinity, health, sexuality, membership of a professional organisation, data relating to criminal convictions and personal data in relation to a prohibition imposed for unlawful behaviour or harassment.

- The Wbp has a broad understanding of terms such as ‘health’ or ‘beliefs’. For instance, ‘health data’ includes: ‘all information regarding a person’s physical or mental health’. The explanatory notes state that even the fact that a person is ill, is health data, although the fact in itself says nothing about the nature of the illness.

2. Information on the financial or economic situation of the person involved.
3. (Other) information that could lead to stigmatisation or exclusion of the person involved. This includes, for example, information on professional achievements or relationship problems.
4. Information that relates to people from vulnerable groups.
5. (Other) information that could be misused for (identity) fraud. This could include biometric data, copies of identity documents and the Citizen Service Number (BSN).

Separate criterion: processing of the Citizen Service Number (BSN)

As well as the processing of personal data, the processing of the BSN is considered as a separate criterion. Pursuant to article 24 of the Wbp, the BSN is a legal identification number. It should only be used for objectives as described in law. This is because the BSN is the ultimate link between personal data, both within and between organisations.

Citizen Service Number (BSN): which assurance levels are appropriate?

Assurance level: none

- The BSN is not processed.

Assurance level: low

- The BSN is only specified by the user.
- It may be linked back (possibly in combination with a limited amount of other personal data no higher than class 1 (see table), for example a name, so that you are certain of the correctness of the BSN provided).
- This also includes the ‘implicit’ specification of the BSN and other situations where the user exchanges the BSN with you, but the BSN is not visible. This happens, for instance, in DigiD or via the future BSN link-register (see table).

Assurance level: substantial

- The BSN is processed in conjunction with additional personal data.

What is the BSN link-register?

The BSN link-register (BSN-K) is a government provision that links authentication devices from private and public parties to the BSN of the holder of the authentication device. The identifiers that are processed, exchanged and possibly displayed are pseudonyms but have the BSN as their basis for public service providers. The BSN may be 'invisible' for the citizens using the service, but it does become available for you, the service provider.

The system of pseudonymisation through the BSN link-register complies with all relevant requirements for privacy-friendly use of pseudonyms. The BSN-K does not fall within the scope of electronic service provision and is therefore not within the scope of this guide.

Nature of personal data: which assurance levels are appropriate?

Assurance level: none

Class 0 personal data

- No personal data are processed.
- It concerns public personal information that is generally considered to not pose any risk to the person involved. This could include information from phonebooks, brochures and websites.

Assurance level: low

Class I personal data (basic)

- There is a limited amount of (non-special) personal information for each individual.
- There is one type of record, for instance one membership, employment relationship or customer relationship.

Assurance level: substantial

Class II personal data (increased risk)

- Special personal data are used (as mentioned in article 16 of the Wpb) or financial-economic data of the person involved.

Assurance level: high

Class III personal data (high risk)

- Information from investigative agencies is used, information from DNA databases, information that is subject to special, statutory confidentiality, and data that are subject to professional confidentiality (such as medical information) pursuant to article 9, section 4 of the Wbp.

Ad 2: Is there an appropriate security level in view of the risks surrounding (the nature of) processing?

As indicated, we want to assess whether the nature of processing leads to extra risks, that in turn lead to the requirement for a higher assurance level. Analogous to the AV23, we consider the following factors:

1. Does your service process a large volume of data per individual (several records, several objectives), so that loss and unlawful processing could lead to excessive invasion of privacy? For example, the leaking of a complete medical file usually leads to a larger invasion than the leaking of a repeat prescription.
2. Objective or objectives for processing the personal data. The more far-reaching the decisions made based on the processed personal data, the more significant the impact from loss or unlawful processing.
3. The extent to which the information is suitable for misuse. Mainly the possibility of identity fraud.

If one of these issues is relevant for information up to class 2, then we opt for the assurance level that suits the next higher class (see table).

4.1.2 What are the legal consequences of the use of your service?

The use of your service may have legal consequences. This applies if your service has a legal basis and leads to legal acts. This could include a decision that is liable to objections and appeals. But your service may also merely involve factual acts. This could include information supply. In that case, your service is not aimed at legal consequences.

There is a third type of service. This is aimed at factual acts, such as registering refuse containers to a name and address. However, this may lead to legal consequences: the information may be used for enforcement. In that case, it involves indirect legal consequences.

Legal consequence: which assurance levels are appropriate?

Assurance level: none

- There are no legal consequences.

Assurance level: low

- There are indirect legal consequences.

Assurance level: substantial or high

- There are legal consequences.

4.1.3 Does your service make changes to key register data?

Data in a key register form a special category. This could include information from the civil registry, birth registration and the municipal key register of the residential address. If these data are processed, the consequences could be significant. After all, this information is shared with a large group of recipients.

Authentic information is part of key register data. Each record or mutation thereof should be handled with the utmost security and accuracy, as recipients have to adopt this authentic information without further checks, and be able to trust it (the so-called mandatory use).

The assurance level that applies to this category is usually ‘high’. However, there is an exception. Does it involve data that are intended for inclusion in a key register, but that are still subject to additional checks by the organisation responsible for the key register? Then, in certain cases, the ‘substantial’ level applies to this data processing. This is the case for many processes by the Civil Registry, for example.

Key register data: which assurance levels are appropriate?

Assurance level: substantial

- Authentic or non-authentic information is provided or changes are provided, to be included in key registers. These mutations provided are still subject to checks.

Assurance level: high

- Authentic information is created, amended or functionally terminated in key registers.
- Other information is directly recorded or amended in key registers, without further checks.

4.1.4 How substantial is the economic interest of your service?

Is there any economic interest involved in your service? Or is it possible for economic damage to occur due to erroneous identification, identity fraud or incorrect processing of data? This could include financial damage due to misuse or fraud, loss of money or economic position, liability, unauthorised persons gaining access to competition-sensitive information (potential 'lost order') or price-sensitive information being leaked.

There are always two levels to be considered here:
- The economic damage as suffered by the individual citizen or the individual business that use a government's service. For the determination of the desired level at individual level, you must assume the potential damage.
- The economic damage suffered at system level, which means the citizens or businesses together or the government as a whole. Empirical data can be used in order to determine this.

The highest of both estimations is decisive for the assurance level to be adopted.

Economic interest: which assurance levels are appropriate?

Assurance level: none
- The economic interest is nil. You do not anticipate any economic damage from an erroneous identification or authentication.

Assurance level: low
- The economic interest is minor for the person or organisation involved. The consequences of an erroneous identification or authentication are unpleasant, but do not lead to forced adaptations to activities or social wellbeing.
- This could include damages (caused by erroneous identification or authentication) of less than 2 per cent of the annual turnover of the organisation involved or less than 20 per cent of the monthly income of the person involved.

Assurance level: substantial
- The economic interest is moderate: it involves larger interests on an individual level or limited business interests. Any damage is controllable and has a temporary effect on the activities of the organisation or person.
- This could include damages (caused by erroneous identification or authentication) of 10 per cent of the annual turnover of the organisation involved or the total of a monthly income of the person involved.

Assurance level: high

- The economic interest is high: it involves interests to an extent that the unaltered continued existence of the organisation or at the same level of social wellbeing for the person involved is severely threatened.
- This could include damages (caused by erroneous identification, identity fraud or authentication) the size of the annual turnover (or annual budget) of the organisation involved or an annual income of the person involved.

4.1.5 How substantial is the public interest of your service?

Earlier, we made the interest of the individual citizen or the individual business a key focus. This concerns the public interests. In this, we can distinguish between publicity issues and political unrest on the one hand and social disruption on the other hand.

Public interest: which assurance levels are appropriate?

In case of risk of publicity issues (due to damaged public confidence in the service provision)

Assurance level: low

- There are complaints, there are reports in the media.

Assurance level: substantial

- For example, there is intervention from the National Ombudsman and there are questions in parliament.

Assurance level: high

- Those that are politically accountable face problems.

In case of risk of social disruption

Assurance level: low

- There are disturbances that can be solved by one organisation.

Assurance level: substantial

- There are disturbances that demand coordinated action from several organisations (often public and private).

Assurance level: high

- There is a state of emergency. For example, there are disturbances that require emergency response measures outside of the normal legal and financial frameworks.

4.2 Reference scenario

The classification model in this guide is very appropriate if your service processes and IT are of average vulnerability. But what is that average vulnerability? The assumptions on this are made more explicit below. They form the reference scenario.

Deviations to the reference scenario

There are deviations to the reference scenario that often occur. We call these adjustment factors. They could lead to you having to opt for a different assurance level or to the necessity for carrying out a complete risk analysis.

Assumptions for het reference scenario

Assumptions on services and users

- You offer one or more interactive, online services for citizens, businesses or both. Whether this involves application-application traffic and return flows.
- Citizens make use of your service(s) for themselves or allow authorised people to do so on their behalf. Employees make use of your service(s) for the business where they are employed.
- There is a clear demarcation of the type of regulation and the type of service you provide.

Assumptions on IT security and privacy

- You have operating management systems for information security and the protection of personal data.
- Your service has an implemented and up-to-date IT security plan in place. This plan is based on standard practice, a specific risk analysis or both.
- There is knowledge of which personal data are processed specifically for your service (and possible regulation). The type of processing actions is also clear. (See chapter 4.1.1 for personal data and chapter 4.1.3 for data processing within the framework of a key register).

Assumptions on the process behind the regulation and service

- You comply with the prevailing legislation for your service.
- The user is authenticated prior to access to your service. This identity is used in the subsequent process.
- You can take additional measures to verify the identity of the user, but this does not extend past back-office checks. You do not request the user to provide extra guarantee of his/her identity.
- Do you offer a service that comprises a decision by an administrative body? In that case, the decision will always be communicated to the party involved. If necessary, other parties involved will also be notified. This may take place through a channel different from your service.

4.3 Adjustment factors

The reference scenario on which the classification model is based does not give the same result in every situation. There are both risk-reducing and risk-increasing factors.

Risk-reducing factors

Risk-reducing factors occur particularly when there are extra process steps that reduce the risk. Based on this, you may have sufficient cause to opt for a lower assurance level than is indicated by the classification model.

Five situations with risk-reducing factors

1. The follow-up process requires the party involved to report and identify themselves in person (with a legal identity document and BSN). This way, you are certain that he/she actually wants to make use of your service with the details he/she has supplied.
2. There is feedback for changes to information or for (intended) decisions through a channel different from your service. Please note: a different channel could also be a different electronic channel. Confirming a transaction (or its result) from a government website via the Berichtenbox (Message Box) therefore qualifies in that case. Of course, the other channel must make use of availability information that is separate from the transaction in question. Confirming a transaction on a government website with feedback via an e-mail, where the e-mail address is provided in the transaction explicitly does not qualify.
3. The follow-up process includes information or documents not connected to your service that prove that the user is actually involved with your service and has given permission.
4. There is continuous and active monitoring of your service. This prevents your service from being approached by the same user many times in a short space of time. This also highlights suspicious user patterns that point to fraud. It is also risk-reducing if you maintain risk profiles or enforcement profiles.
5. Is the economic interest decisive for the assurance level of your service? And does it involve a financial service? If yes, verification of the account details for payments is risk-reducing.

Assurance level reduction prohibited

Is there a risk-reducing factor for your service? Then you can often lower the assurance level by one step. This is not possible if:

- legal requirements determine the assurance level (form requirements for signing, for example);
- the assurance level was initially at 1. You cannot move back to 0. After all, risk-reducing factors cannot change the nature of the information. Measures will always be necessary to guarantee the reliability and confidentiality of personal data.

Risk-increasing factors

Risk-increasing factors relate to the context of your service. This could include political or administrative sensitivity or image. In this guide, we do not impose a higher assurance level, but recommend that you carry out a complete risk analysis.

Four situations for a complete risk analysis

1. Your service is associated with a substantial political, administrative or image risk.
2. It is difficult to determine the risk, as the direct consequences of an incident are limited. At the same time, the potential consequential damage is substantial.
3. Your service is at high risk of large-scale misuse by organised crime. This is especially the case with a combination of mass processes, limited control options and when (large-scale) misuse is highly profitable.
4. Your service is an attractive prospect for terror organisations or foreign intelligence services.

In many cases, the above coincides with services where the QuickScan BIR also indicates a complete risk analysis should be carried out. However, the list above is decisive on whether you should also carry out a complete risk analysis for the determination of the assurance level of authentication.

4.4 Examples of services and assurance levels

Which services and assurance levels belong together?
Below are some examples that follow the criteria above.[14]

Services	Authentication level
• Anonymous visits to government websites • Municipal local services (such as notifications of public spaces or requests for refuse containers) • Access to WOZ valuation	No requirements
• Registering for personalised portals • Logging permit • Event permit • Environmental permit for private individuals • Reporting of minor offences (such as bicycle theft)	Low
• Registration of death (by an undertaker) • Notification of intended marriage or registered partnership (by partners) • Registration of birth (by parent) • License application for sex businesses • Pre-completed tax returns • Business tax returns • Subsidy application • Application for financial allowance • Reporting of serious offences (such as assault or domestic violence)	Substantial
• Consulting a medical file • Consulting decisions by administrative bodies with (medical) information • Consulting criminal information • Request for screening on behalf of a third party	High

[14] WOZ valuations are considered to be publicly available information.

5 Authorisations

Which assurance level is appropriate?

5.1 What is it actually about?

There are many situations where citizens or businesses are represented by someone else. Such a representative is authorised to act on behalf of the citizen or business. An authorisation has no effect on the assurance level of an individual service in principle: after all, it doesn't change the nature of the service. There are special circumstances, such as guardianship, receivership and attribute disclosure for example, where specific considerations and checks are requested. We will not go into this any further. This chapter deals with authorisations in the general sense of the word.

It is important to recognise an authorised representative without doubt. After all, you would not want representatives to log in using the citizen's or business's own log in details, as this would be as if they themselves are those citizens or businesses. The representatives could also use those log in details for other things, although this wasn't the intention. Therefore, it is better to strive for only explicitly recorded and recognisable authorisation. The authorised representative is then recorded in an authorisation register. It holds information on which acting party is authorised to carry out which activities on behalf of which citizen or business, as well as the scope of the authority to act. This authorisation register also provides authorisation declarations. This is done via digital messages stating that the acting – authorised – party is in fact authorised to use the electronic service in question on behalf of the intended citizen or business.

Example: digital tax returns
Digital authorisations are partly possible with DigiD Authorisations. But digital authorisation options are not in place everywhere yet, although they are necessary in the digital world. Especially in view of the trend where the government is increasingly making digital data processing by citizens and businesses mandatory. One example is the, by now, more or less mandatory digital tax return. The National Ombudsman poses that 'people who are having difficulties with digitalisation should be able to receive adequate support' (see also chapter 2.2.4). As of 2016, there are no adequate authorisation facilitiesfor social support workers for tax returns (the so-called HUBAs: help with tax returns). Logius is in the process of working on implementation of this.

5.2 What do authorisations mean for an individual service?

As indicated, whether you are dealing with a citizen or a business, or with their representative, the assurance level for your individual service doesn't change.

However, authorisation registers are necessary for situations where you, as the service provider, do not manage the authorisations. An authorisation register records authorisations and issues authorisation declarations with a suitable assurance level. Authorisation registers should be set up so that the desired assurance level for the process of recording authorisations is safeguarded. The starting point for this are the eIDAS assurance levels.

It is important to recognise that authorisations are recorded in a chain where not all the steps are necessarily digital. In those cases, the administrator of the authorisation register will look after the conversion to a digital authorisation declaration.

It is also possible that authorisation registers are not used. You, the service provider, will then receive paper issues of authorisations or via a digitally certified message.

5.3 What does authorisation mean in practice?

For the setup of the individual service, the assurance level as per eIDAS and the guidelines by the Data Protection Authority (AP) (see chapter 4.3) are valid. Recording the authorisations should occur at no less than the same assurance level. Therefore, as a service provider, you should check whether the authentication is accompanied by an authorisation declaration at no less than the same assurance level. Whether or not there is authorisation is up to the user of the service.

5.4 Other focus areas: misuse and fraud

The risk of misuse or fraud can increase in case of representation. After all, fraudsters can claim or register fraudulent authorisations. This risk should be intercepted. Firstly, by the necessity to prove authorisation at the required assurance level each time a service is used. Secondly, by imposing correct requirement on registration and the use of authorisations. These are listed in the set of agreements for Idensys and eHerkenning, for example.

If a citizen wishes to authorise someone (or a business) to represent him or her, then registering an authorisation should be a relatively low-threshold matter. If the threshold is too high, the chances of passing on their own log in details and other unacceptable behaviour remain high. Take this into consideration if representation plays a part in the service you offer.

Furthermore, as the service provider, you must notify the persons involved of the use of authorisations. This provides the citizen or business involved with a concrete insight into who uses government services on his/her behalf.
This could include an opt-out option as offered by the Dutch Tax and Customs Administration. The citizen or business receives a letter containing a notification that tax intermediary X wishes to submit the returns on behalf of that person. This letter (Returns Service Notification – SBA) informs the citizen/business of this fact and offers the option to make corrections simply by returning part of the letter to Logius using the prepaid addressed envelope. Logius manages the authorisations on behalf of the Dutch Tax and Customs Administration.

6 Application-application traffic

How do you manage service provision without human intervention?

6.1 What is it actually about?

Digital service provision is increasingly carried out without human intervention. For instance, an automated system can use a service from another automated system. This is called application-application traffic. One example of this is Digipoort.

The following characteristics are typical for application-application traffic:

- There is no human intervention.
- It concerns communicating applications, the natural person is not in the picture.
- It often concerns considerable volumes (total or individual flows of messages).

6.2 Protection methods

Both the channel and the content of this traffic can be protected:

- By securing the channel, a 'safe tunnel' is created between the organisation providing the service and the organisation using the service. Both sides are aware where the other side of the tunnel is located. The tunnel itself ensures safe transport of data. These cannot be read or altered by a third party whilst in the tunnel.
- It is also possible to protect the content: the message itself. For this purpose, a message is signed and certified and often also encrypted. It ensures that messages can be relayed with end-to-end security. It makes it impossible to read or alter the message during transport.

Table 1 lists some notable differences between channel security and content security.

***Table 1.** Channel security versus content security*

Channel security	Content security
Universal More types of content, often also from several applications, can use the same channel.	**Specific** Each content has its own security.
Transient You cannot tell from the content that it was safely transported.	**Permanent proof** Characteristics are linked to the content that prove authenticity.
Secure up to first intermediate destination The traffic is protected from the tunnel entrance up to the point where the tunnel 'surfaces'.	**End-to-end security** Secure traffic to prior and future chain parties is also possible.

Factually, digital certificates are the security standard for both channel and content security. They are often combined. Digital certificates provide more security than other forms of protection, such as passwords.

Secured traffic with digital certificates

SBR
Digital certificates are now widely used for Standard Business Reporting (SBR). For example, businesses or intermediaries use SBR for tax returns or for submitting annual accounts. To this end, their systems communicate with those of the government via Digipoort. The traffic is secured with a PKIoverheid (services) certificate.

Communication with key registers
Government bodies typically have dozens of these certificates and often unique certificates for each connection for communication with the various key registers, which is done through digi-links. In this process, PKIoverheid certificates are used.

6.3 What does this mean for application of the classification model?

This guide is less useful for application-application traffic. You would use digital certificates for this in practice. The only remaining question is how reliable those certificates should be. In practice, you should opt for PKIoverheid services server certificates, both for the security of the channel and the encryption of the contents. PKIoverheid is also the mandatory standard in accordance with the State Baseline Information Security (BIR) and associated baselines.

Focus points for digital certificates

Government bodies are very dependent on digital certificates, both for channel security and for protection of the contents. Three important focus points for you, the service provider:

- Ensure that you have spare certificates of alternative certificate service providers available for critical applications;
- Ensure that you have appointed more than one authorised certificate manager within your organisation. This is an authorised person who can, for example, request new certificates from various certificate service providers and can revoke old certificates.
- Prevent a single-point-of-failure to prevent that in case of failure, an entire process or chain comes to a halt.

7 Return flows

As a service provider, what are you doing with the digital messages you send?

7.1 What is it actually about?

As a service provider, you not only receive digital messages from users. You can also approach or respond to the users via digital channels. This interaction also takes place between applications. This is called the 'return flow', an important part of the digital communication. This could include:

- *E-mail* – you send a digital message to the e-mail address of a natural person.
- *A web portal or Berichtenbox* – you place messages in an individual, secured web portal or in a Berichtenbox and notify the citizen (via text message or e-mail) that there is a message waiting for them.
- *Application-application traffic* – you run return flows via application-application traffic, directly to the organisation involved or to an intermediary (see chapter 6).

7.2 What does this mean for an individual service?

The Dutch General Administrative Law Act (Awb) contains regulations on digital traffic. The Awb stipulates that both you and the addressee must ensure that the return message actually reaches the addressee. You should arrange for a reliable and secure medium, the citizen or the business has to check their own post. For return messages, it is important that the following matters are in hand:

- Ensure that the message or document reaches the addressee.
- Prevent unauthorised persons accessing the message or the document.
- Ensure that the addressee is able to verify that the message or document genuinely originates from you.

The Awb allows the citizen or business to decide whether they want to communicate via digital means. If they choose to do so, they should be available via this method.
In other words: within the Awb, normal post and the electronic channel are regarded as equivalent. However, the electronic traffic is already mandatory at several points and it is expected that this shift will continue. See the textbox 'Shifts with legal consequences' on page **52**.

E-mail

E-mail is generally not suitable for return flows. There are several reasons for this:

- Citizens and businesses don't necessarily maintain an up-to-date e-mail address. This means that return flows may not arrive at the correct address.
- In many respects, e-mail is a less reliable and secure medium. Messages have to be encrypted for sensitive information. In order to do this, you require a digital certificate from the citizen or the business. However, there is no incentive for citizens and businesses to provide a current certificate.
- You have to go above and beyond to prove that your message really is from you. One of the options to achieve this is to certify the messages (see textbox 'Reliable documents from the government' in paragraph 7.3).

E-mail is reasonably suitable for feedback of data with low sensitivity. This could include general information or service announcements. However, the e-mail address must have recently been provided or confirmed by the citizen or business for this to be effective.

Web portal and Berichtenbox

As a service provider, you can place return messages on your own web portal. You provide access through DigiD, for instance. Service providers increasingly use the generic Berichtenbox provision (part of MijnOverheid). This is where addressees open and read (return) messages from the government in a safe environment. They receive a notification when new messages are waiting in the Berichtenbox. There is also a Berichtenbox for businesses.

How certain is it that the correct person has access to the (return) messages? The Berichtenbox for citizens offers assurance level 'Low', as the authentication for the Berichtenbox takes place via DigiD. The addressee can be pretty sure that a message is from the government, as the source is either the Berichtenbox or another trusted government service.
Access to the Berichtenbox for businesses is also set to level 'Low', although it is at eHerkenning level 2+, which is higher than the applied DigiD level for citizens.

The remaining weak point is that you are dependent on the availability of an up-to-date e-mail address or mobile phone number to notify the citizen or business of new messages. As these are merely notification messages, it is a less substantial problem than if you exclusively choose e-mail for return messages. Of course, the citizen also benefits from good registration of such contact information, but it is a focus point nonetheless.

Application-application traffic

When you send a return message directly to the organisation involved, the channel security ensures the desired assurance. As the reachability of the addressee is arranged inherently well for application-application links, chances are that the message actually arrives. The channel security furthermore ensures that outsiders cannot access the message. An application-application link can therefore be very reliable.

In case of representation, you will usually want to notify both the intermediary and the party involved. Some intermediaries also provide digital services to the clients they represent. In such cases you could consider conducting the return flow to the citizen or business via the intermediary's digital channel. But ultimately, the party involved decides how he/she wants to be digitally reachable.

7.3 What does this mean for the application of the classification model?

You can apply the classification model to the return flows. When doing so, you consider the data in the return message. Which assurance level is appropriate? The service used for sending return messages should have the same assurance level as a minimum. You have the following options:

- E-mail can only be used for messages with a maximum assurance level of 'low'.
- Whether a web portal or Berichtenbox is suitable depends on the assurance level of authentication for the Berichtenbox. For now, that level is 'low'. This level should also be sufficient for your specific return messages.
- The (channel) security for application-application traffic is in place properly, as it often uses PKIoverheid (services) server certificates. Is there another destination for the return message? Then the situation is more complex and you should carry out an extensive risk analysis.

Shifts with legal consequences

From issue obligation to fetch obligation

It used to be customary that the government sent legally important documents to the receiver. The government had an 'issue obligation'. This is slowly making way for a model where citizens and businesses have a 'fetch obligation'.

Technical interpretations shift the meanings of issuing and fetching. Today, fetching may mean that a citizen is obliged to open and deal with his/her post. Tomorrow, it may mean that the citizen has to log in to a mailbox system from the government or another service 'from the cloud'.

From optional channel to mandatory channel

A second shift concerns the status of digital service provision. Currently, the Awb and the electronic administrative traffic Act include an 'equivalence principle': citizens and government have to make available both a paper channel and a digital channel.

However, there is an undeniable movement towards 'digital, unless'. It is becoming the norm, in fact. For example, the digital channel has been made mandatory for tax returns. A good example is the obligation of electronic profit return for businesses and the more recent abolition of the blue envelope for citizens with the introduction of the Tax Office Electronic Message Exchange Act.

This will probably also change the legal situation regarding the return flow. However, it is as yet still unclear how this will happen.

Important: certify your documents

A citizen or business will often want to establish whether certain documents are actually from an authority, such as the government. This could include digital documents that have to be submitted elsewhere as official documents, such as decisions, extracts, official declarations or public notices. Citizens and businesses want to determine with certainty that the documents are official.

Seals and time stamps

The fact that the government digitally certifies these types of documents benefits the legal security of citizens and businesses. Especially if the documents serve as evidence for a third party. Governments are not doing this enough as yet. If they do, they use a digital signature from their organisation or from an employee. eIDAS is introducing special trust services for this purpose. It is obvious that these should be used. It involves:

- *Electronic seals* serve as proof that a digital document has been issued by a government organisation, for example. This guarantees both the origin and the integrity of the document. As well as for documents, electronic seals can also be used for the authentication of digital documents that must be protected against alteration or replacement by unauthorised persons, such as program codes.
- *Electronic time stamps* serve as proof that a document (or collection of data) was in existence at a certain point in time. They do not carry guarantees on the origin of the document, nor the integrity and correctness of the information.

eIDAS requirements

Both electronic seals and electronic time stamps are subject to requirements in eIDAS. Advanced and qualified electronic seals are acknowledged, entirely analogue to electronic signatures. For electronic time stamps, standard and qualified electronic time stamps are acknowledged.

High assurance level

If you wish to certify documents, it seems obvious that you would use electronic seals and time stamps with a high assurance level. This could include an advanced electronic seal based on a qualified certificate. Or an electronic time stamp on a qualified level.

Standard formats

For interoperability, it is wise to work with the standard formats PadES, XAdES, CAdES and ASiC for signing documents. These formats are also listed in the EU decision 2011/130 and the Implementation Decree (EU) 2015/1506. They have been classed as the formats that you, as a government body, have to accept as a minimum.

Validation

As well as certifying your documents, you must also ensure that the receiver can validate the certified documents online. This is sometimes done automatically with the existing programmes, sometimes you will need to ensure a validation service is in place. If you utilise a non-standard format for signing and sealing documents, you are legally obliged to offer a free validation service.

Registered delivery

Finally, eIDAS also deals with services for electronically registered delivery. This means that the identities of both the sender and the receiver are guaranteed, as well as delivery to the receiver. The existence of a safe and reliable communication channel with citizens is important. Registered delivery fits nicely into that objective.

Carrier
1:27 PM
100%
Password
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Emergency
Cancel

8 Single Sign-On

What does user-friendliness mean for safety and reliability?

8.1 What is it actually about?

Single sign-on (SSO), is the option for users to gain access to various services via one authentication (provision). The user logs in once at the first service and does not have to confirm his/her identity again for other services. There are possible measures required if the user switches from a service by one provider to a service by another provider.

An example of single sign-on

MijnOverheid offers access to an entire set of (combined) data and services by various (government) organisations when a citizen logs in, such as the Key Person Register (BRP), the RDW (Traffic Services) and the Pension Register. MijnRVO.nl offers businesses one authentication (after registration) for access to many specific services such as the manure register, many subsidy services and various fisheries options.

An important term for one-time log-in is the federation. Essentially, the federation is a group of services that jointly use an SSO solution. It varies from one individual organisation with several digital services to, for example, a government-wide portal.

There are federations that only maintain one assurance level. If they facilitate different assurance levels, the user is able to switch from one service to another service with a higher assurance level. New or additional authentication is required in that case.

Closely related to one-time log-in is one-time log off (single sign-off). This provides the user with the certainty that he/she ends the open sessions and access to services in one action.

8.2 Individual service perspective

In case of one-time log-in, it is important for you, the service provider, to know the assurance level at which the authentication took place and whether it is still valid. However, there are more focus points for one-time log-in. What does federation participation involve? What is SSO like from a user perspective? We will look at this in more depth in paragraph 8.4.

8.3 What does this mean for the application of the classification model?

One-time log-in does not shine new light on the criteria and considerations of the classification model. In fact, one-time log-in is an authentication device. You have to determine the assurance level this occurs at on the basis of the classification model.

8.4 Other focus areas

One-time log-in is subject to several focus points that are important for you, as the service provider. We will list the two main points.

8.4.1 Being part of a federation

If you opt for SSO, you will find yourself in a federation. There are some things to take into consideration before you choose to participate.

1. Can you influence the design and operation of the federation? You are no longer alone in deciding how authentication is done.
2. The assurance level may be higher or lower than what is required for your service. This may occur if the federation maintains one single assurance level.
3. What about the customer's user-friendliness? A federation with various assurance levels may offer customised authentication for the service, but not as much user-friendliness. When the user switches to a service with a higher assurance level, he/she has to authenticate himself/herself again. This negates the advantage of logging in once via SSO.

Low threshold of the Social Insurance Bank

As a service provider, you determine the desired assurance level for your service. Is a lower assurance level available through SSO? Then you can refuse access to your service. But you could also adjust your service in such a way that a lower assurance level suffices, for instance by taking mitigating measures further along your process.

A good example of a low-threshold solution is the service by the Social Insurance Bank (SVB), users only need DigiD Basis. However, one consequence is that users are not able to arrange all matters online or that the SVB has to send a confirmation letter after finalising an online transaction.

8.4.2 User perspective

From the perspective of the user, logging in once can lead to confusion. If he/she has opened various sessions and one-time log out is not available, the sessions are not ended immediately. It may be unclear which sessions are still open, which may cause extra security risks.

As a service provider, you could consider the effects of one-time logging in and out for the user. You could take measures at the level of your own organisation. For instance, you could explain to users what one-time log-in means and how it can be managed. You could also formulate wishes and requirements for the federation, for better and safer services for the user.

9 Signature

Do you require an electronic signature for your service?

9.1 Introduction

We are used to signing documents frequently in the physical world. Is this also required in digital service provision?

This chapter answers the following:

1. Signing and the electronic signature, what does this mean? (See paragraph 9.2)
2. Do you, the service provider, need electronic signatures? If yes, which type and how reliable? (See paragraph 9.3)
3. Other questions, including:
   - What does eIDAS do internationally? (See paragraph 9.4.1)
   - Are you obliged to accept electronic signatures? If yes, which? (See paragraph 9.4.2)
   - Do you need to provide the signature capability for citizens and businesses, or can this be outsourced to signing services? (See paragraph 9.4.3)

9.2 Signing and the electronic signature, what does that actually mean?

The aim of signing is to (legally) bind citizens or businesses to transactions or (a collection of) documents.[15] Several factors are important:

- The signatory *understands* the relevant content and the consequences of signing.
- He/she *confirms* the relevant content.
- The signature provides *proof* of the above for a third party.

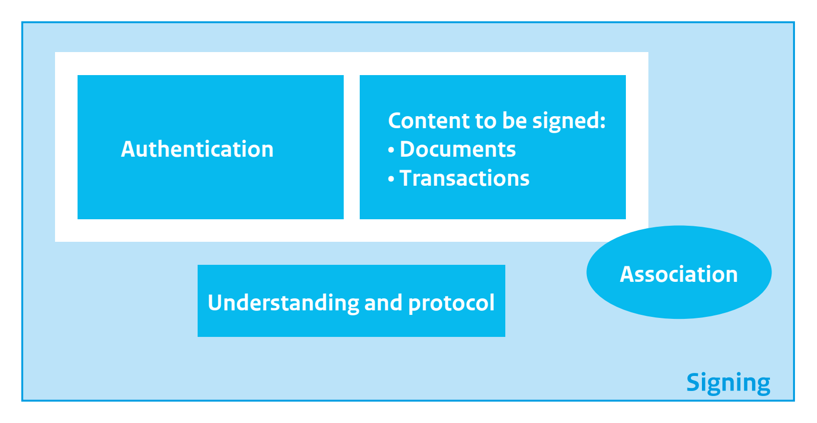
This legal binding requires a certain protocol that clearly marks the moment of signing. It reduces the chance of hasty signing.

[15] Legislation also often requires a record in writing. But this does not necessarily mean a signature or a physical document. 'In writing' means 'composed in characters'.

What does a signature actually 'do'?

The understanding and confirmation of a transaction or document should lead to a so-called association. An association means that a connection has reliably been established between: the signed document, the identification and authentication of the signatory and the service or the process from where the document originated and was signed. An electronic signature is a set of data that are logically associated with the document (or other information) to be signed. The abovementioned association also becomes provable through a signature. The conclusive force depends on the type of electronic signature used and – deeper down – the power of the underlying authentication and association mechanisms.

So in the use of signatures, identification, authentication, and association play an important role. This is what it looks like in a diagram:



Understanding and protocol are not an implicit part of the *association.* But they do implicitly belong to a certain service or signing situation.

Electronic signatures in eIDAS

An electronic signature is a set of data that is associated with the signed document or the signed information. It represents the signatory's identity and the authenticity of the signed document or the signed information.

The eIDAS regulation lists the following definition:
An electronic signature is any data in electronic form that are attached to or logically associated with other electronic data and that are used by the signatory for signing.

Types of electronic signatures
eIDAS distinguishes three types of electronic signature, namely:
1. Electronic signatures,
2. Advanced electronic signatures and
3. Qualified electronic signatures.

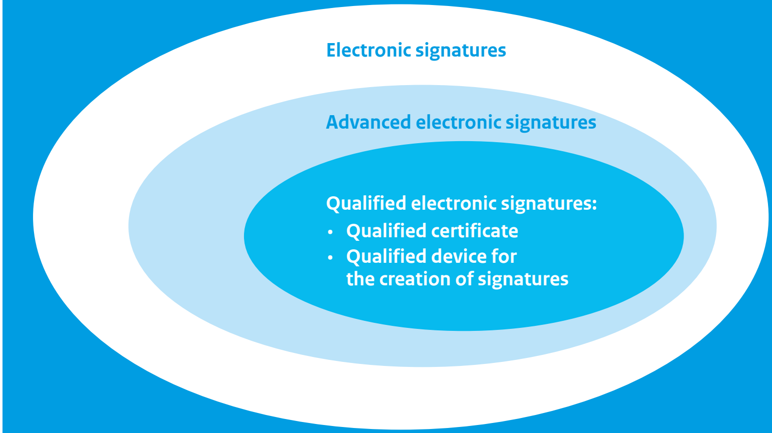
1. Electronic signature (see article 3.10 of the eIDAS regulation)
An electronic signature must meet the requirements that are implicitly stated in the definition. In other words, it should concern electronic data that are attached to other electronic data by the signatory with the aim of confirming and recording the will of the signatory. No further requirements are imposed on how the electronic signature is created or on the conclusive force it offers.

2. Advanced electronic signature (see articles 3.11 and 26 of the regulation)
The advanced electronic signature:
- is uniquely attached to the signatory;
- makes identification of the signatory possible;
- is created with data that the signatory can use under his/her sole control, with a high trust level;
- is attached to the signatory's information in such a way, that later changes to this information can be detected.

The definition of advanced electronic signature is irrespective of a certain technology. However, the digital signature commonly used is based on the technology by Public Key Infrastructure (PKI).

3. Qualified electronic signature (see articles 3.12, 28 and 29 of the regulation)
The qualified electronic signature is an advanced electronic signature. But most of all, a qualified electronic signature is
- based on a qualified certificate and
- uses a device qualified for such purpose, for the creation of electronic signatures.

Figure 4. *The three types of electronic signatures. Some electronic signatures are advanced. Some advanced electronic signatures are qualified.*


Electronic signatures
Advanced electronic signatures
Qualified electronic signatures:
• Qualified certificate
• Qualified device for the creation of signatures

A *qualified certificate* is a confirmation of the signatory's identity, attached to data that can verify the electronic signature. This qualified certificate is issued by a qualified provider of trust services, after thorough identity verification. To this end, a qualified service provider is certified beforehand on the basis of European standards. The identity verification of the signatory comprises a face-to-face check, or safely relies on a previous face-to-face check. The exact requirements for the qualified certificate are listed in appendix I of the eIDAS regulation. It is too extensive to include it here. Just as all other suppliers of all qualified trust services, issuers of qualified certificates must be qualified themselves. This means that as an organisation, they must also be under previous supervision by the Telecom Agency.

The data used to create the electronic signature are secured against leaks, copying or misuse by third parties by way of a *qualified device*. Such a device could be a smartcard or USB crypto-token, but other resources are also possible.
In addition, the eIDAS regulation offers space for other methods to expand the storage and management of encryption material. It is worth mentioning that it is also possible to store and manage cryptographic keys elsewhere for instance, which paves the way for broader diversity of technical solutions and service provision (see also 9.4.3 on signature services). This increased space is most obvious from consideration 55 in the regulation. In addition, the regulations on the sole control have been subtly changed in article 26 (see part c of the requirements for the advanced signature). Controls no longer imply physical possession of the data used for signing. Personal control (through logical partitioning) of the remote online environment where signing takes place will also suffice.

Validity of electronic signatures

- For the purpose of legal consequences, the qualified electronic signature is equal to the handwritten signature. (See article 25, part 2 of the eIDAS regulation.)
- Other electronic signatures may also have legal consequences and serve as proof. The sole fact that they are electronic or don't comply with the requirements for qualified electronic signatures, does not affect this.

In the Netherlands, the Civil Code (article 15a) includes a broader equivalence of the electronic signature and the handwritten signature. This creates more concrete effect to the second point. The BW (Dutch Civil Code) refers to electronic signatures (as intended in the eIDAS regulation, article 3) and states that, as well as the qualified signatures, other electronic signatures also carry the same legal consequences as the handwritten signature, as long as they are sufficiently reliable for the service they are applied to.
In processes and transactions subject to less significant legal consequences or other consequences, a standard electronic signature will suffice (an electronic signature that is not an advanced electronic signature), whilst transactions where the consequences are more significant, an advanced or qualified electronic signature is required.

Importance of the signing process and its environment

The electronic signature does not only concern the identification and authentication of the signatory, but also the question whether the signed document or signed information are authentic and genuine. What exactly was signed and (in which form) has the signatory (actually) seen it? This is why the process and the environment in which signing takes place are also important. They are also decisive for the level of reliability, for the acceptance of the signature and for the verification by an independent party, such as a judge or arbitrator in case of a dispute.

For the purpose of conclusive force for a judge or arbitrator, important questions could be:

- How probable is it that the electronic signature was actually added by the signatory to whom this signature is attributed? (Was it actually the signatory himself/herself?)
- Has the signing process been designed in such a way that the signatory is aware of the content and the consequences of what he/she has signed?
- Has a reliable time indication been used at the moment of signing, such as a time stamp for example?
- What is the power of the association mechanism, so does the electronic signature actually belong to the signed information or the signed document?

9.3 Which electronic signatures do you need as a service provider?

Do you actually need electronic signatures?

The question remains whether you actually need electronic signatures for your service provision. Consider the following points:

- Do you want citizens and businesses to understand and confirm what they commit to?
- Do you want independent proof that a person has signed a certain document or certain information? Or do you consider a log-in by a managed computer system to be sufficient, even if it renders the compiled proof more complex? If so, you could also summarise the information to be signed and have it reconfirmed by the signatory, if necessary with an extra authentication action.
- Does legislation force you to use an electronic signature?
- Do you provide services to citizens and businesses from other EU member states for which an electronic signature has to be accepted in order to access the service?

Analogy with paper-based situation

Do you request a signature in your traditional ‘paper’ service provision? This does not automatically mean that this should also be the case in your electronic service provision. This is because a signature can serve a different function on paper. Ceremonial for instance, to make the signatory aware that he/she is committing to something. Or to confirm the identity provided, as in authentication for electronic service provision. So be careful using the paper situation as a lead. First, consider the aim and the value of the paper-based signature before you translate this signing process directly into an electronic signature.

What types of electronic signature are appropriate for your service provision?

The same criteria as in chapter 4 are relevant for this question. However, There is one difference. Other than in case of authentication, users cannot access (privacy-sensitive) information with their electronic signature. This is why one central question remains for electronic signatures:

'Does the service provision record or amend personal data (varying in nature) in registries?'

The considerations here are comparable with those in chapter 4. It concerns the following:

1. If personal data are processed:
   a. what is the nature of the data that requires protection? Are special data also processed? Is the Citizen Service Number (BSN) processed? Are benefits or financial information processed?
   b. what are the relevant characteristics of the processing operation itself?
2. What are the legal consequences of the use of the service?
3. Does the service make changes to key register data?
4. How substantial is the economic interest of your service?
5. How substantial is the public interest of your service?

You should also consider how powerful the desired conclusive force of the electronic signature should be, both short and long term. It is important whether you can undo (reversibility) or sanction the consequences of a false declaration by a citizen or business (see textboxes with example cases).

You can use the table below to select an electronic signature.

Criteria	Types of electronic signatures
• Personal data maximum class 1 • BSN processing solely through submission by citizen and linked back to class I personal data. • Possible indirect legal consequences • No modification to key register • Minor economic interest • Public interest low • Limited conclusive force required	Standard signature
• Personal data maximum class 2 • Aggravating factor for personal data in addition to class 1 • BSN processing with additional personal data • Direct legal consequences • Limited effect from amendment of key register data • Moderate economic interest • Moderate public interest • Significant conclusive force required	Advanced electronic signatures
• Personal data class 3 • Aggravating factor for personal data in addition to class 2 • BSN processing with additional personal data • Substantial effect from amendment of key register data • Significant economic interest • Significant public interest • Highest possible conclusive force required	Qualified electronic signature

Please note: A more reliable type of electronic signature can also be applied in all situations where a less reliable type of signature is already sufficient. The qualified electronic signature can therefore be applied in all situations.

Example case: subsidy providers

Imagine you are a service provider and your organisation provides subsidies to Dutch businesses upon application. Businesses create an application in which they declare various facts. Based on these facts, you award a subsidy. These subsidies are modest in comparison with the turnover of the businesses, no more than several thousand euros.

The businesses have to sign the application and the supporting declaration about the facts. This means the signatory is bound, which means it is difficult for him/her to later deny any possible false declarations.

Reversibility and sanctionability?

In this process, there is a high degree of reversibility: an incorrectly awarded subsidy can usually be recovered from the business. The sanctionability is important in this case. However, the signature is only the first step. After this, there is written feedback of the application and decision.

Which type of signature?

The type of data and economic interest indicates an advanced electronic signature. But due to the written feedback of the application and decision, the risk is further reduced. Based on this, even a standard electronic signature would suffice.

Example case: employment agencies and payroll businesses

Employment agencies and payroll businesses have been increasingly managing the entire process of agreements with employees digitally.

Reversibility and sanctionability?

In this case, the consequences are easily reversible.

Which type of signature?

The significant economic interest would indicate a qualified electronic signature. Due to good reversibility and sanctionability, an advanced electronic signature would also suffice.

9.4 Other questions about electronic signatures

9.4.1 International aspects

eIDAS arranges several cross-border matters:

- The qualified electronic signature is uniformly defined in all member states. The essential requirements for this qualified electronic signatures have been determined EU-wide. Moreover, the legal status of this signature is equal in all member states
- For cross-border traffic, it is not permitted to demand a level higher than the qualified electronic signature.
  There is no standardised level above the 'qualified' level, for that matter.
- Do you, the service provider, require an advanced electronic signature or stamp as a minimum? Then you have to accept electronic signatures and stamps at this level and higher assurance levels (see the eIDAS regulation, article 27). Furthermore, according to eIDAS you are obliged to be able to receive and process specific electronic signature formats, such as the XAdES, PAdES and CAdES and the ASiC standards (see the EU implementation decree 2015/1506).

9.4.2 Are you obliged to accept electronic signatures?

Signature within the Services Directive

You might not be aware, but since the introduction of the Services Directive (2009), you can already receive permit applications with an electronic signature. You are not allowed to refuse this electronic signature.

Prescribed signatures

The State government is able to prescribe the electronic signature, in accordance with the Dutch General Administrative Law Act (second paragraph of article 2:16). A different administrative body can do this if it has regulatory authority in its own regulation. Reasons could be the use of digital information or the legal relationship between the signatory and the administrative body.

Is the electronic signature mandatory? Then you may have to deal with extra requirements regarding security and reliability of the signature. This could include the level of authentication for the creation of the electronic signature. Or the independence and security of the signature. There could also be additional requirements for the standard electronic signature that are created on a tablet or touch screen.

International signatures

Do you deal with an advanced electronic signature based on a qualified certificate? Or with a qualified electronic signature? These are valid throughout the EU. You must accept these, especially if they comply with the standardised formats for electronic signatures (CAdES, PAdES, XAdES and ASiC). Besides, you cannot just refuse other electronic signatures any longer, taking into account that electronic signatures cannot be denied legal consequences only because they are electronic or because they do not comply with certain assurance requirements. So the signature has to be accepted unless there are good reasons not to do so. As a service provider, you are able to demand a certain level of electronic signature for your electronic service.

9.4.3 Can you use signing services for signing?

Traditionally, the signatory himself/herself (or the organisation he/she signs for) provides his/her electronic signature. For instance, the signatory has purchased a certificate from a *trust service provider* and he/she has ensured there is software for signing. He/she also follows a suitable process for this, which prevents incorrect or hasty signing.

This is the traditional implementation model, but it is also clear that the implementation burden is considerable. This could be problematic, especially for citizens or small businesses. This is why we can see the emergence of signing services, who implement the signing process and create the electronic signature. The signatory authenticates himself/herself to the signing service who, in turn, look after the association in interaction with the user (and his authentication device, if necessary). This way, the signatory only has to have one authentication device.

Space is given to signing services within eHerkenning and Idensys too, as long as they comply with certain requirements. What's more, the eIDAS regulation offers space to bring encryption material for creating an electronic signature under the central management of a signing service as well. By the way, it is not *necessary* that a signing service also manages the encryption and codes that are used for the creation of a signature, but it is good to realise that the eIDAS regulation does not prohibit this.

The use of a signing service can save the signatory and his/her organisation time and effort. This is also true for you, the service provider: a signing service can ensure that electronic signatures you receive are of the correct reliability and in the right format and that the signing process was thorough.

If it concerns electronic signatures you receive as a service provider, then the following options are available:

- Do nothing. You only indicate the type of signatures you wish to receive. The party that has to sign something should then ensure that it has the signature your organisation requires.
- Referral. You refer to independent signing services. The party that has to sign something can then contact the signing service if they do not have their own electronic signature.
- Do it yourself. You implement a signing service yourself for your electronic service provision. The party that has to sign something can then do the signing in your digital environment, whereby your organisation is responsible for the signature.
- Outsourcing. You contract a signing service for your electronic service provision. The party that has to sign something can use a signing service within your digital environment, managed by an external party.

This should include some focus points:

- The above raises the question about who will foot the bill for a signing service. Is it the service provider or should the costs be borne by the signatory. This will mostly depend on the specific application.
- The 'do it yourself' option implies that you, the service provider, become party to the signing process of the citizens or businesses. Attention to independent positioning of the signing service is preferred, in order to be in a position of power in case of a signing dispute.
- It concerns a relatively new form of service provision. You would be advised to gain a deeper understanding of the requirements you wish to attach to such service provision, if you wish to use a signing service.

Overall, signing services are an interesting form of service provision, that reduces the implementation burden of the electronic signature. As it concerns a relatively new form of service provision, it would be sensible to take an in-depth look at the service options from a standpoint that takes into account the needs of your organisation.

Appendix 1 Relevant laws and regulations

1 eIDAS regulation

The European eIDAS regulation came into force on 1 July 2016.[16] In addition and in line with the above, Implementation Decree 2015/1502[17] offers a legal framework for assurance levels. These have formed the basis of this (fourth) version of the guide. The eIDAS regulation is a European regulation that has direct effect in the member states, which includes the Netherlands. As such, a regulation supersedes national legislation. Dutch legislation must not deviate from the regulation. A large number of implementation aspects are set out in the eIDAS Implementation Act, which is under parliamentary scrutiny at the time of creating this Guide. The European Guideline 1999/93 on electronic signatures will be revoked as a result of the eIDAS regulation. Most of the matters set out are now included in part 2 (Trust Services) of the regulation.

The Regulation is made up of two parts:
1. Electronic identification (authentication)
2. Trust Services (including electronic signatures) Below are explanatory notes for each part.

Part 1. Electronic authentication device

One of the most important objectives of the eIDAS regulation is that it enables genuine cross-border electronic service. To this aim, a mandatory mutual recognition of electronic identities between EU member states will come into force from September 2018. Implementation Decree 2015/1502 contains quite detailed provisions about which requirements the different levels have to comply with.
Finally, the eIDAS regulation also describes the technical interoperability, so that links between national systems for electronic identification and authentication can be successfully implemented. Member states are obliged to implement the required technical provisions for this.

The above is expected to finally enable cross-border electronic service provision, where the erstwhile Electronic Signatures Guidelines proved to be insufficient.

[16] *http://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX%3A32014R0910*

[17] IMPLEMENTATION DECREE (EU) 2015/1502 BY THE COMMISSION of 8 September 2015 for determining minimum technical specifications and procedures regarding the assurance level for electronic identification device pursuant to article 8, paragraph 3 of Decree (EU) no. 910/2014 by the European Parliament and the Council regarding electronic identification and trust services for electronic transactions within the internal market.

The mutual recognition between member states concerns systems for electronic identification and internal authentication devices at levels 'substantial' and 'high'. To this end, member states must notify Brussels and the other member states of systems and other devices that are to be qualified for cross-border use.

In order to achieve cross-border access to electronic services, electronic identification devices must comply with communal requirements. However, these requirements will also largely be applicable to electronic identification devices within the Netherlands. Below is a list of permissible concessions.

The requirements are:

- Services that require 'substantial' or 'high', must be accessible to private parties (citizens and businesses) from other member states. A party from another member state should use the authentication device from the other member state. It goes without saying that this device must have the same eIDAS level. The eIDAS requirements are therefore in force nationally when it comes to authentication device at level 'substantial' or 'high'.
- Devices must be issued under identical conditions (mutual recognition). Pursuant to consideration 14 of the eIDAS regulation, the principle of mutual recognition only applies to authentication of an online service. Access to these online services and the actual provision thereof to the applicant should be closely linked to the right to use such services at the conditions set out in national legislation. National legislation may prohibit access to e-services. There are limits to access refusal, such as non-discrimination regulations. This means that a citizen from a different member state who has access to the UWV website using his/her authentication device, is not automatically eligible for benefits in the Netherlands. The electronic access naturally does not alter other rights and obligations.
- Devices with eIDAS level 'low' are also defined in the regulation. There is no automatic European recognition for these devices. However, states can opt to allow access to specific devices from other member states that have eIDAS level 'low'. This has to be explicitly arranged.

Part 2. Trust Services

The Electronic Signatures Act (Weh) implemented the Guideline 1999/93/EG on a joint framework for electronic signatures. From 1 July 2016, this Guideline expired and the Trust Services section from the eIDAS regulation is now in force.

The Guideline is implemented in the Netherlands via the Electronic Signatures Act (Weh). The Weh added articles 15a and 15b to Book 3 of the Civil Code. The Trust Services section of eIDAS replaces the current Electronic Signatures Act and adds other trust services to it.
In order to arrange specific matters from the eIDAS regulation, but also to avoid duplicity within national legislation of the provisions in the regulation, a proposal for an eIDAS Implementation Act is currently under parliamentary scrutiny. Article 15a on the electronic signature will have a slightly different interpretation in this legislative proposal for the eIDAS Implementation Act (see also chapter 9). Article 15b will be abolished. Several other Dutch laws, including the telecommunication Act, will also be amended.

As well as electronic signatures, the Regulation also sets out a number of other trust services:

1. Electronic seals
2. Electronic time stamps
3. Electronic delivery services
4. Website certificates

For this, see also the 2nd textbox on page 52 of this guide.

Starting principle in the Regulation is that the provider of trust services located in one member state is not obstructed in the provision of its trust services in another member state. The Regulation sets out, among other things, the requirements for provision of these on the market, the monitoring specification, a reporting obligation in case of security breaches, the legal consequences and the cross-border recognition thereof. So-called qualified variants are acknowledged in these trust services. Extra strict requirements apply to qualified trust services, as well as a more stringent (a priori) supervisory regime than for non-qualified trust services.

2 The Dutch General Administrative Law Act

Through the electronic administrative traffic Act (Webv), a section 2.3 has been added to the General Administrative Law Act (Awb). This section 2.3 contains general rules on the electronic exchange between citizens and administrative bodies.
By now, the electronic traffic Act has also come into force with the administrative court, an amendment of the Awb that arranges the electronic traffic with the administrative court by declaring section 2.3 of the Awb equally applicable to it. Below is a brief explanation of the Webv articles that have been included in section 2.3 of the General Administrative Law Act.

The general outline of the Webv can be summarised as follows:

- The regulations on electronic traffic with administrative bodies apply to all e-services that are included in the scope of this guide.
- Electronic traffic is regarded as equivalent to conventional traffic.
- The Webv regulations stipulate that electronic traffic is offered parallel to the option to use services on paper or by visiting a counter. Mandatory use of electronic traffic as a sole channel requires an explicit legal basis.
- Electronic traffic and electronic sending of messages, as intended in these regulations, must have a broad meaning and comprises websites, e-mail, electronic transactions, web services, etc.
- The Webv lays down conditions that must be observed in the provision of e-services. These are conditions regarding:
  - the fact that the sender and the receiver (so both administrative body and citizen) must both have communicated previously that they are electronically reachable;
  - reliability and confidentiality of the traffic, taking into account the nature and the content of the message and its objective. Of course, this aspect is important for classifying the required assurance level;
  - requirements for signing;
  - times of sending and receipt of electronic traffic.

These main points will be elaborated on below.

Article 2:13 Awb

This article sets out that the traffic between citizen and administrative body may contain electronic messages (first paragraph). It also determines the span of this option. Electronic traffic must comply with the regulations in section 2.3. What this means specifically is included in the explanation of the other articles in section 2.3.

Article 2.13 concerns dispatch in the broadest sense of the word. In any case, this term is broader than when used in everyday speech. It concerns notifying, informing, sending, forwarding, returning, communicating, announcing, confirming, ordering, expressing, submitting, etc.

'Sending via electronic means' includes any form of electronic data exchange with another party. It concerns, for example, sending an e-mail as well as posting an article on a website. It concerns traffic from the government to citizens and businesses as well as traffic towards the government.

In fact, article 2:13 is the basis for electronic execution of all types of services and processes between government and citizen or business. This option can only be excluded by legal measure (which means through a law, General Order in Council (AMvB) or ministerial decree) (second paragraph, section a). Up to now, there is no known legislation that explicitly excludes the option of electronic traffic. Appendix 2 lists several examples of formulations in legislation that cannot be considered exclusion of electronic traffic.

A second exception of the principle that traffic between citizen and administrative body may take place electronically, is the situation where a procedural requirement opposes electronic dispatch of messages (second paragraph, section b). Specific examples of this for the Webv legal proposal Are not mentioned by the Explanatory Memorandum (MvT). However, there is mention of some cases where procedural requirements that seem to lead to the use of paper, also allow electronic 'dispatch', such as 'per letter' (could also mean e-mail) or 'attach' (could also mean publication on a site). So, it is unlikely that this exception will hinder electronic traffic. However, appendix 2 does list several (legal) procedural requirements that could possibly hinder electronic traffic.

Article 2:14 Awb

The first paragraph sets out that the administrative body can only communicate electronically with the citizen if the citizen has made it known that he/she is reachable in that manner. There is no provision for how this notification by the citizen should take place. The mere sending of an e-mail by a citizen to a government organisation will generally not be sufficient; it cannot be assumed that the citizen remains reachable at that address. Appendix 2 lists several examples of suitable notification methods.

The need for notification reflects the principle of equivalence in the Webv: (the increase of) the electronic traffic should not be to the detriment of those who cannot use it. For those people, the government should remain reachable via the conventional method. The second paragraph sets out that messages that have not been addressed to one or more addressees (public announcements, notification of public inspection of land-use plans, etc.) should not solely be sent electronically. This means that, as well as electronic public notification, the announcement must also take place in a government information letter or a newspaper, magazine, free local paper or other suitable method (in accordance with article 3:12 and 3:42 Awb). The documents should also be made available for inspection in the conventional manner (i.e. at the council offices).

The third paragraph of article 2:14 lists another important principle of the electronic administrative traffic Act, which is reliability and confidentiality of the message exchange. When an administrative body sends a message electronically, it should occur in a sufficiently reliable and secure manner, in view of the nature and content of the message and its objective.

The MvT for the Webv distinguishes three levels of reliability and confidentiality:

- *Maximum reliability and confidentiality*
  This applies if the security takes place entirely in accordance with the maximum (technical) capabilities.
- *Adequate reliability and confidentiality*
  This applies if the security is equal to a situation where only conventional traffic is used.
- *Proforma reliability and confidentiality*
  This applies if the security is only one step away from providing no protection at all. This could include an (electronic) ‘no entry’ notification.

For the record: these three measures are not directly linked to the three levels of reliability as set out by the eIDAS regulation.

The legislator aims to reflect the so-called general principles of proper IT use through the requirement for reliability and confidentiality. This comprises the principles of authenticity, integrity, non-repudiation, transparency, availability, flexibility and confidentiality. Specifically, these principles can be safeguarded, for example, with technology that enables an electronic signature with a time stamp or with the help of cryptographic technology (encryption).

The legislator states that the middle option of adequate reliability and confidentiality should be sought. Similar safeguards to those available for 'paper traffic' should be offered. The legislator does not wish to require a higher degree of reliability and confidentiality in the electronic situation than is the case with conventional communication.

Level 'high' involves maximum reliability and confidentiality, for instance to enable access to patient information.[18] As such, the eIDAS levels and the devices available in the Netherlands form a interpretation of the open standard from the Awb.

Despite the cohesion in the standards for reliability at national and EU levels, it is difficult to say when there is an adequate level of reliability and confidentiality in practice. The main rule is that the nature and content of a message and its objective determine the level of reliability and confidentiality required. For instance, issuing a permit should be subject to stricter requirements than issuing general information. In a practical sense, this means that the standard for reliable and confidential communication will have to be reflected in the policy of the relevant administrative body. The application of this guide and the implementation of the required assurance level for own services is part of such a policy.

[18] See the report 'Patient authentication [Patientauthenticatie]' by J. Krabben (PrivacyCare) and T. Hooghiemstra (PBLQ), commissioned by the VWS minister: *https://www.rijksoverheid.nl/documenten/rapporten/2016/08/25/bijlage-vi-onderzoek-betrouwbaarheidsniveau-patientauthenticatie*

Article 2:15 Awb

The first paragraph of article 2:15 forms the mirror image, as it were, of the first paragraph of article 2:14. It sets out that the administrative body must also have indicated to be reachable electronically. This so-called opening of the electronic channel by the administrative body can occur both in a general regulation and in a notification to one or more addressees.
The administrative body can impose further requirements to the use of the electronic channel (first paragraph, second sentence), with the aim of uniform treatment and safe data traffic. For instance, an administrative body can insist a certain electronic mail address is used. It could also include more technical requirements, such as the use of certain software or certain electronic (intelligent) forms. For mass-processes, a specific channel for a specific type of message with specific requirements can be opened. This may also include the determination of assurance levels for certain processes or services. The further requirement can be established in consultation with stakeholders. The agreements resulting from consultation can be laid down in an exchange protocol. An exchange protocol contains, among other things, the norms and standards necessary for communication and message definitions that are required for the automatic processing of data.

Opening the electronic channel will almost always necessitate further requirements for actual implementation of the electronic traffic. Therefore, the further requirements will often relate to physical provisions to support effective and efficient message traffic aimed at the entire processing route. This is why they are often not laid down in a decision or regulation by the administrative body. If an administrative body maintains an equivalence principle, and if the electronic message traffic is an addition to the conventional method, the requirements can be considered part of the policy. If a citizen or business does not want to conform, he/she has the option to use the conventional (written) method. If the electronic message traffic is explicitly made mandatory, excluding the conventional paper route, it would be reasonable to include these further requirements in the general binding regulations. The mandatory character and the consequences that may be attached to non-compliance of those regulations justify a legal basis.

Assurance requirements for the electronic route can be along the same lines. If these requirements are limited to appointing a reliability level, it can be considered policy interpretation, whereby the user is given the option to choose a device for identification and authentication that complies with this assurance level. If a specific device is prescribed for identification and authentication, this option is no longer available and a legal basis for the obligation is logical.

The second and third paragraph of article 2:15 list grounds for refusal for electronic messages. The administrative body can refuse a message if processing it would lead to unacceptable imposition, or if the reliability and confidentiality of this message are insufficiently safeguarded. Sufficient reliability and confidentiality are taken to mean the same as in article 2:14, paragraph three.

Article 2:16

The reference in article 2:16 Awb to the requirements for an electronic signature in article 3:15a, second up to and including sixth paragraph, has been abolished as these regulations have also seized to exist in the Civil Code. The regulation sets out its own rules on the subjects that were laid down in these articles. The implementation act will include a new paragraph stipulating that a signature must be sufficiently reliable for the process it is used in and that legally valid signatures can be required, either with specific requirements or not. Exceptions are the advanced signature and the qualified signature, as the regulation sets out exhaustive requirements for these.

Article 2:17

This article sets out the times of sending and receipt of an electronic message. This is important for determining the start of the term of objection or appeal.

The first paragraph lays down that the dispatch time by a administrative body counts as the time at which the message reaches a system for which the administrative body bears no liability. If the administrative body and the addressee use the same system for data processing, this is the moment at which it becomes accessible to the addressee. This provision applies to a situation where the parties involved actually use the same system. One example is the electronic dispatch of documents between the Municipal Executive and the Municipal Council. This is not likely to apply to the traffic between government and citizen. In accordance with the second paragraph, the moment of receipt by an administrative body counts as the time that a citizen’s message has reached the administrative body’s system.

3 The Dutch Personal Data Protection Act

The Personal Data Protection Act (Wbp) (updated as per 1 January 2016) was replaced on 1 July 2016 by the General Data Protection Regulation, applicable from 25 May 2018. An implementation decree, such as for eIDAS, is to follow. The following still takes the Wbp into account.

The Wbp is applicable in situations where (electronic) traffic takes place between government and citizens/businesses. Article 1, part a of the Wbp defines personal data as: any fact regarding an identified or identifiable natural person. For example:

- Surnames, first names
- Personal e-mail address
- Telephone number
- BSN
- Personal certificate

In articles 6 up to and including 14, the Wbp sets out strict requirements for gathering, processing and storing personal data. These requirements include:

- Processing must take place for the purpose of execution of statutory tasks or in case of explicit permission from the person whose data is processed.
- Processing must comply with the aim for which the data was obtained.
- Those responsible for processing must provide suitable technical and organisational measures for the prevention of loss or unlawful processing of personal data.

Wbp article 16 sets out extra requirements for special personal data, such as information on a person's religion or beliefs, race, political beliefs, health, sexuality, and information on membership of a professional organisation, and data relating to criminal convictions. For these personal data, a prohibition for processing applies.

The articles 17 up to and including 22 determine which bodies are allowed to process such personal data and under which conditions. An exception to the processing prohibition also applies here if there is a legal basis for processing or in case the person involved has given explicit permission for processing (article 23). Moreover, the Personal Data Authority can grant dispensation for processing these details. It is important that personal data does not just include the identifying characteristics, but also the combined information that can be retraced to a certain person, such as information on the financial-economic or personal situation. For this reason, telephone numbers, car license plates, postcodes with house numbers and the BSN can be defined as personal data.

The Personal Data Authority has issued Guidelines for the Protection Of Personal Data. See paragraph 4.3 of the main text.

Providers of trust services are excluded from the reporting obligation pursuant to Wbp article 34a (data leaks reporting obligation), as laid down in article 10 of the proposed implementation act relating to the execution of the eIDAS regulation. The reporting obligation for providers of trust services to the Personal Data Authority has been set out in the legal proposal via an amendment to the Telecommunications Act. This offers the option of specifically taking into account the direct meaning of the regulation.

4 Dutch legislation relating to information security

As well as the Wbp, the Civil Service (ministries and directly subordinate services) have to comply with regulations on information security. These are particularly aimed at the measures that are taken internally in this area by (part of) a ministry. However, its application may be decisive for determining the assurance level for a certain service. The measures for information security in the back office could lead to a lower assurance level being sufficient at the 'gate'.

As discussed in chapter 2, the attention for information security has increased significantly over the last few years. This is in line with social developments and the strong growth of the use of online services. This has led to various regulations, standards and guidelines. This guide is specifically aimed at assurance levels required for online services from the government. It is assumed that other aspects of these services comply with the relevant prevailing standards. Chapter 2 already mentioned the DigiD ICT Security Assessment Standard, together with underlying guidelines by the NCSC. Which other regulations are important for a government organisation?

The Information Security Regulations 2007 (VIR 2007) apply to parts of the State. This sets out, among other things, that information security must be part of the standard control cycle and the responsibility of the line management. The tactical set of standards Civil Service Baseline Information (BIR2012) gives further information on how this should be interpreted. Similar documents have been created for municipalities and various other authorities. These will be included in a government-wide baseline. All these regulations are actually an application of the ISO 27001/27002 standard for the government. This standard is part of the *'comply or explain'* list by the Standardisation Forum[19]. This means that all governments have to deal with these regulations one way or another.

Various matters laid down for the purpose of information security can be reused for the implementation of this classification. Therefore, classification is also very suitable for synchronised implementation with a Quickscan BIR. The guide looks in depth at the interaction with citizens in e-services. In addition, the Quickscan BIR casts a broad view on internal aspects, such as the IT systems used in a process and the required availability. If the Quickscan BIR shows that a higher risk applies to a certain service than what is covered by the BIR, it follows too that the simplified risk analysis proposed here is insufficient. Therefore, regulations for information security and this classification are therefore both required and complement one another.

Civil Service Information Security Regulation 2007 (VIR 2007)

One of the intended regulations is the Civil Service Information Security Regulation 2007 Decree. In this decree, information security means the following: the process of determining the required reliability of information systems in terms of confidentiality, availability and integrity, as well as taking, maintaining and monitoring a cohesive package of additional measures. Information security is a line responsibility and forms part of the quality assurance for business and management processes and the supporting information systems. As a result of the decree, the secretary general is responsible for the determination, propagation and substantiation of the information security policy of his ministry.
The tasks imposed on the line management by the decree as a result are:

- Determining the assurance requirements of the information systems based on an explicit risk assessment.
- Applying this guide and subsequently recording the resulting assessment are part of this. This guide only looks at the assurance requirements, expressed in levels, for electronic access by external users or users of a service.
- Determining, implementing and propagating the measures that arise from the assurance requirements.

[19] Insofar as application of ISO 27001/27002 and government regulations derived from it and based on 'comply or explain' can still be qualified, it follows that the new version of the ICT Security Guidelines for Web Application from the NCSC imposes a similar level, together with the existing technical measures, also for organisational measures. It is to be expected that this will become an inescapable regulation in the next version of the DigiD security standard. The same expectation also applies to requirements that will be imposed on users of the Idensys system.

- Determining that the measures taken demonstrably coincide with the assurance requirements and that there is compliance with these measures.
- For government-wide provisions for electronic access, such as DigiD, PKIoverheid and eHerkenning, it applies that this demonstrable compliance stems from the assurance level issued by service providers responsible for these provisions.
- Evaluating and adjusting, where necessary, the entirety of assurance requirements and security measures periodically.

Civil Service Baseline Information Security (BIR)

As well as the process-oriented VIR, a formulation for the civil service is now in existence and was determined in 2012. The BIR is aimed at content. It concerns the mutual measure objectives and measures, and is based on the ISO 27001 and 27002 guidelines, with additional specific measures for the state. Just as in the VIR, it deals with availability, integrity and confidentiality.

The level of the baseline is Departmentally Confidential and Wbp Risk class II increased (roughly analogue to class II as presented in chapter 4). The BIR is deemed to be mandatory, with a note that the applicable measures can be selected.

Data Security Regulations for Special Information (VIR) Decree (VIR-BI)

As well as the VIR, there is a separate decree for special information. This decree set out how the civil service should deal with so-called confidential information in the sense of state secrets. The lowest class is departmentally confidential, which is also the level of a baseline offered by BIR. However, the VIR-BI is limited to the confidentiality aspect.

In cases where a section of the civil service is a user of electronic services (for instance the application for a permit by a ministry), this decree could be directly applicable to information that is provided for that purpose.

An analogy is offered for the remaining cases. The state secret classification is outside of the scope of this guide. The departmentally confidential classification is usual for tender information, for instance, and can be understood as an analogy for what is considered seriously sensitive from a competitive or economic viewpoint in the business world.

As well as the BIR, there are baselines for other governments (BIG, IBI, BIWA). However, these are not so much legal obligations but administrative agreements.

5 The Dutch Citizen Service Number General Provisions Act

The citizen service number (BSN) is an important provision for the identification and authentication of persons. The Citizen Service Number General Provisions Act lays down rules about issuing and utilising this number, among other things.

The act sets out that all government bodies are allowed to use the number when processing personal data for their public service, without the need for further legislation. For use outside of the circle of government bodies, a specific legal basis remains necessary.

It may be necessary to lay down the public service in a law as such (for instance, if it concerns a new task that will involve processing of the BSN).

The BSN management provision could be asked electronically whether a certain person was assigned a citizen service number and if yes, which citizen service number. This way, the citizen service number of a certain person can be screened. The management provision could also be asked which person a certain citizen service number relates to. This can be used to check whether the citizen service number provided by a person actually belongs to the person involved, for instance through comparing the information with a (Dutch or foreign) identity document.

The ways of ascertaining do not rest on the appearance of the citizen service number on an identity document, but are applicable to all persons assigned a citizen service number. By linking the citizen service number to DigiD, the citizen can identify himself/ herself electronically in a reliable manner.

6 The Dutch Code of Civil Procedure

As a result of the eIDAS regulation, the sentence 'an electronic signature that complies with the provisions of article 15a, first and second paragraph, of Book 3 of the Civil Code' as it appears in article 1072b, third paragraph, of the Code of Civil Procedure is replaced with: 'a qualified signature as laid down in article 3, part 12, of regulation (EU) no. 910/2014 from the European Parliament and the Council of 23 July 2014 regarding electronic identification and trust services for electronic transactions on the internal market and repealing guideline 1999/93/EG (PbEU 2014, L 257).'

Article 156a of the Code of Civil Procedure (Rv) contains provisions on the creation of electronic private documents. Private documents are documents that can or must serve as proof of legal transactions. This could also include documents that have to be submitted for a permit application. This is why this article is also relevant for electronic services.

For the adoption of article 156a Rv, private documents had to be drafted on paper in order to be able to provide the desired proof. The addition of the article enables the creation and provision of electronic insurance policies, among other things. The article is as follows:

Article 156a

1. *Private documents can be drafted in ways other than in writing, in such a manner that it enables the person for whom the document provides proof, to save or store the document in a manner that makes it accessible for future use during a period adapted to the purpose for which it was intended, and that enables unaltered reproduction of the contents of the document.*

2. *The legal obligation to supply a private document can only be fulfilled in a manner not in writing with express permission from the person to whom the document must be provided. Permission also applies to the provision of an amended private document, as long as it has not been revoked. The provision in the first sentence of this paragraph does not apply unless the document has also been signed by the person to whom the document legally has to be provided.*

Article 156a, first paragraph, Rv requires that the manner of drafting a document enables an unaltered reproduction of the document's contents. This formulation is derived from a term durable medium in the Financial Supervision Act.

In article 1:1 of that act, durable medium is defined as: ‘a resource that enables a person to save or store information personally addressed to him/her in a manner that makes it accessible for future use during a period adapted to the purpose for which it was intended, and that enables unaltered reproduction of the contents of this saved information.’ This demand does not stretch to the person drafting the document having to guarantee an unaltered reproduction of the saved information. The reason stated for this is that he/she has no influence on the choice of device (CD-ROM, USB-stick) used by the person for whom the document is created. For signing electronic private documents, an electronic signature pursuant to article 3:15a of the Civil Code is generally required. The question whether a normal, advanced or qualified signature is required for a certain private document depends on the purpose of the information and all other circumstances of the case. This is why there is no provision in article 156a Rv for which signature is required.

Other than for the electronic signature, the act does not contain a general provision that indicates in which circumstances an electronic signature has the same legal consequences as a paper document (a written document). However, there is an indication for specifically described situations where the act imposes the requirement for a document to be in writing, that this can also be complied with via the electronic route. Examples of this are article 6:227a Civil Code on the creation of agreements and article 1021 Rv on the arbitration agreement.

Article 156a Rv only sets out the conditions under which private documents can originate.

Appendix 2 Examples of interpretation of legal frameworks and conversion of papers to the electronic situation

This appendix lists examples of interpretation of the requirements from the statutory rules regarding electronic traffic between government and citizens. In addition, there is an indication of how the paper situation is translated to the electronic situation, based on the general legal framework as described in appendix 1 and some extraordinary laws for arranging electronic traffic with the government.

1 Sending electronic messages

Article 2:13 Awb explains 'dispatch by electronic route' as any form of electronic data exchange with another party. This offers many more options for communication between government and citizen than with the conventional paper traffic. Examples are:

- Sending and receiving fax messages or e-mails with substantive information. Automated message exchange (for example a tax return or annual accounts in the XBRL standard).
- Completion of a form in a web portal. Also, when the action does not lead to a 'message' visible to the person filling in the form, the form as received by the government organisation can be considered an electronic message pursuant to the meaning in the Awb.
- Sending a message from an application (such as the income tax return via the self-assessment programme downloadable from the Dutch Tax and Customs Administration's website).
- A text message from a government organisation to a citizen or (employee of a) business (such as the text with a one-time authentication code for DigiD).
- A text message from a citizen or (an employee of a) business to a government organisation (such as the text messages used by skippers to notify the Inland Waterways Management from the Amsterdam municipality of a passage).
- A notification via e-mail from a government organisation that a message is waiting on a personal webpage.
- Logging in to a portal to see and/or download a message (such as in the Berichtenbox in *Mijnoverheid.nl*).
- Making available a document on a public website belonging to a government organisation. Please note: this concerns a message that has 'not been aimed at one or more addressees', so the publishing of the information on a site must not be the only method of information provision.
  (This will need to be combined with making the information available at the town hall and/or publication in a free local paper.)
- An app for reporting faults (loose paving tiles, broken play equipment and such) in public spaces.

Examples of 'dispatch of electronic messages' that are probably not covered by article 2:13 Awb:

- A tweet on Twitter (but probably does conform to a resource for distributing 'non-addressed' messages, although not as the sole medium (see appendix 1, section 1, for article 2:14 Awb)).
- An online chat with a civil servant (similar to a telephone conversation).
- A telephone conversation, even though this may be done via Internet in similar messages (Voice over Internet Protocol (VOIP)).

2 Times of sending and receipt

In general, the risk of dispatch of messages via electronic means is with the sender, whether this is a citizen or administrative body. When sending an electronic message to an administrative body, the sender will also have to record whether and when the message was sent. In case of doubt, he/she must check that the message was received. The sender must also actively check status and progression, and keep an eye on whether the message (for example for reasons of technical processability) was refused. If the sender is able to provide a sent report, he/she has generally provided sufficient plausibility that the message was sent. It is then up to the receiver to deny receipt of the message 'in a not incredible manner'.

Article 3:36 of the eIDAS regulation defines a 'service for electronic registered delivery' as: 'a service that makes it possible to send information between third parties via electronic methods and that provides proof relating to the handling of the dispatched information, including proof of sending and receipt of the data, and that protects the dispatched data against the risk of loss, theft, damage or unauthorised alteration.'

The administrative body is not obliged to keep a receipt register or log files. However, if a receipt register is absent, it becomes more difficult for the administrative body to deny 'in a non-incredible manner' that the message was received. In other words: he has to demonstrate convincingly that the message was not received. If the administrative body is successful in doing this, the sender in turn has to make plausible that the message was received nonetheless. The jurisprudence in article 2:17 Awb mainly concerns the sending of messages (for example appeals, applications) via fax or e-mail. However, article 2:17 is also relevant for dispatch via application-application traffic (see chapter 2), and it follows that the sender bears the risk of electronic dispatch. It could also occur that messages are not sent (directly) to the administrative body in application-application traffic (see also chapter 6), but via a generic provision (an electronic post office).

An example of this is Digipoort, for messages from entrepreneurs or their intermediaries (e-invoices, tax returns) to the government. Digipoort sends a confirmation of receipt that serves as proof that 'the message has reached the administrative body's system', as required by article 2:17 Awb. A simple transaction code can suffice, and if there is significant importance, a sealed message with a time stamp can be utilised.

3 Notification

Both the citizen and the government organisation must report that the electronic route is open. Regarding notification by the citizen: 'sufficiently reliable' information must be available about the electronic address where he/she can be reached. Options that satisfy this requirement are:

- Registering in a portal where information can be made available for him/her.
- Actively providing an e-mail address where one is reachable.

The fact that a message was sent to the government organisation from an e-mail address is not by definition valid as sufficient information regarding the electronic reachability.

Also, it is not always true that, on the side of the government organisation, when an electronic address is available once, it provides an open channel for all possible actions. What's more, it cannot be inferred that the electronic route is open in accordance with the Awb, just from the fact that e-mail correspondence took place previously with the government organisation. This requires active notification by the government organisation, for instance through:

- A brochure.
- An announcement in a free local newspaper or on a website, that indicates where on the Internet certain permit applications can be made, where complaints cane be submitted, etc.
- An open-house decision, as made by the Dutch Tax and Customs Administration at the time.

Appendix 3 Terminology

The difference with previous versions of this guide is that this version complies with the definitions in the eIDAS regulation. The different translations of the regulation do not always contain the same definition. This is caused by the various languages.

They are definitions specific to electronic services. This is how we also manage the definitions in the guide. For this reason, a paper passport does not fit the definition of 'authentication method' in this guide. The process where someone's WID document is checked as part of the registration and issuing process of an authentication device is not considered 'authentication'.

Terms:

Term	Explanation
Person	A natural or legal person. A person is a carrier of rights.
Authentication	The confirmation (substantiation) of the (an) identity claimed by a person based on his/her authentication device. The identity claimed is the 'electronic identification' (as defined by eIDAS, see below). This must be able to be confirmed prior to the person receiving access to a service. The latter is called 'authentication'.
Authentication device	A combination of possession, knowledge and characteristics that is personal, which uniquely identifies a certain person and which can be used for authentication for an online service. Based on the verification of possession, knowledge and characteristics, the identity claimed can be proven at a certain assurance level. This 'combination' can be regarded as a 'collection of information' or 'series of data', as laid down by the regulation. As such, these are 'person identification data' as defined in the regulation (see below). 'Data' must be understood in the broadest sense, because an authentication device is 'a material and/or immaterial unit', as laid down by the regulation. One immaterial part of the 'combination' is a password that is only committed to someone's memory. 'Combination' also means that the entire collection must always be used completely and in cohesion, both during the issuing process and during use.
Assurance level	A level of certainty that is offered by trust services in their processes for authentication, registering, managing of authorisations, etc.
Conventional traffic	Traffic, meaning communication and/or messages, whereby messages on paper are sent and received, via personal delivery or with the help of a postal service provider.
Electronic traffic	Traffic that uses e-mail, Internet, short message service (SMS: text messages), fax or other electronic devices for sending and receiving written messages.

Definitions pursuant to article 3 of the eIDAS regulation

The definitions below have been taken verbatim from the Dutch version of the eIDAS regulation (article 3). These definitions are used in this guide exactly as in the regulation.

Definition	Explanation
Electronic identification	The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.
Person identification data	A set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established. Implementation decree 2015/1501 has determined a minimum series of person identification data. There is both a series for natural persons and a series for legal persons. All these details must be checked during the application process of an authentication device. The rules for assessment of the assurance level must always be applied for the entirety of this series. This on the understanding that eIDAS only requires this for cross-border use. For an assurance level of 'Low' and non-cross-border services, concessions can therefore be made.
Relying party	A natural or legal person that relies upon an electronic identification or a trust service.
Signatory	A natural person who creates an electronic signature.
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which are used by the signatory to sign.
Advanced electronic signature	An electronic signature which meets the requirements set out in Article 26 of eIDAS.
Qualified electronic signature	An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.
Electronic signature creation data	Unique data which are used by the signatory to create an electronic signature.
Certificate for electronic signatures	An electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.
Qualified certificate for electronic signatures	A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I.

Definition	Explanation
Trust service	An electronic service normally provided for remuneration which consists of: a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery service and certificates related to those services, or b) the creation, verification and validation of certificates for website authentication, or c) the preservation of electronic signatures, seals or certificates related to those services.
Qualified trust service	A trust service that meets the applicable requirements, as laid down in the eIDAS regulation.
Trust service provider	A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.
Qualified trust service provider	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
Product	Software or hardware, or relevant components of hardware or software, which are intended to be used for the provision of trust services.
Electronic signature creation device	Configured software or hardware used to create an electronic signature.
Electronic document	Any content stored in electronic form, in particular text or sound, visual or audio-visual recording.
Electronic registered delivery service	A service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.
Certificate for website authentication	Attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued.
Validation data	Data that is used to validate an electronic signature or an electronic seal.
Validation	Process of verifying and confirming that an electronic signature or a seal is valid.

Carrier
1:27 PM
100%
Access
Place your finger
Emergency
Cancel

For reuse or citing, please state:
The Standardisation Forum:
assurance levels for digital service provision guide,
a guide for government organisations, November 2016

This brochure is a publication by:

The Standardisation Forum
September 2017 | 104835