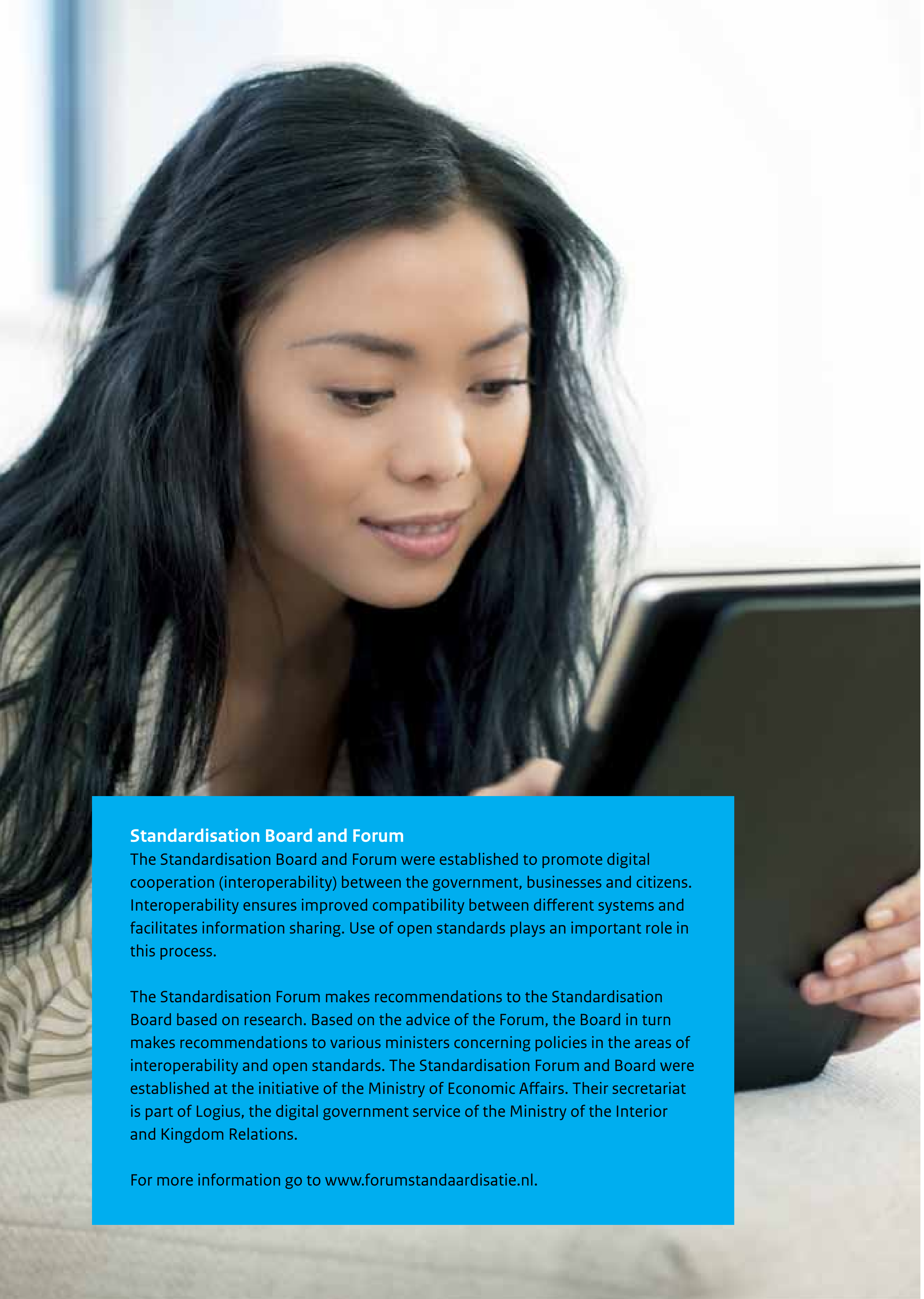
*A guide for government organisations*

# Assurance levels for authentication for electronic government services (version 2)

***The Standardisation Forum***



### Standardisation Board and Forum

The Standardisation Board and Forum were established to promote digital cooperation (interoperability) between the government, businesses and citizens. Interoperability ensures improved compatibility between different systems and facilitates information sharing. Use of open standards plays an important role in this process.

The Standardisation Forum makes recommendations to the Standardisation Board based on research. Based on the advice of the Forum, the Board in turn makes recommendations to various ministers concerning policies in the areas of interoperability and open standards. The Standardisation Forum and Board were established at the initiative of the Ministry of Economic Affairs. Their 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.

# Management summary

## What is the assurance levels guide?

With the intention of achieving a reduction in the administrative burden, improved provision of services and in general a more efficiently operating government, the government is now investing in large-scale comprehensive electronic government services (e-government services) for citizens and businesses. Depending on the nature of the provision of services, the government must more or less be able to rely on who it is they are doing business with. This implies electronic identification and authentication measures.

In the Netherlands there is currently an open standard in effect with respect to the necessary assurance level for identification and authentication of persons and parties using such e-government services. This open standard is laid down in the Dutch General Administrative Law Act (Awb) and within the rules concerning information security. An 'open norm' implies that the relevant requirements have not been concretely defined. The on-going surge of e-services has consequently also increased the need to further supplement this open standard, since it is important that government organisations in similar situations require (and implement) the same levels of reliability and security.

This guidebook provides this supplementary information by giving a simplified risk analysis of the vulnerability of your e-services. This analysis helps you determine how vulnerable they are to misuse or improper use. Based on such a risk assessment one can then choose the desired assurance level for one's e-services (and therewith the authentication tools one's customers use). Situations of authorisation and the consequences of Single Sign Ons are given special consideration.

## How does it work?

The processes behind e-government services in The Netherlands are typically similar in nature and structure. Besides they follow the rules of the Dutch General Administrative Law Act, possibly supplemented with the requirements of domain legislation. This makes it possible to define 'families of related services' and to apply generic systems to assess and consolidate risks.

The system of this guidebook assumes an assessment of the value at stake, according to a number of objective (or objectifiable) criteria and interests. Examples of this are legal requirements, the nature of the data exchanged (e.g. is personal data involved) and the economic or social interest associated with a certain service or process.

An estimate can subsequently be made of the potential damage if the service is used unlawfully. Based on this simplified risk analysis the service is finally classified at a certain assurance level.

## Who is it for?

This guidebook is written for government organisations providing e-services to citizens and businesses. It may involve a web portal with e-services for citizens and/or businesses, but also return flows or application-to-application traffic. This guide offers a foundation for dialogue between policy-makers, (process) architects and information security personnel for the implementation of e-services and back office processes.

This booklet will additionally offer managers insight into the rationale behind the determination of assurance levels, so that they may make a well-informed decision.

## What is it meant for?

The choice for an assurance level for a certain e-service, and therefore also the application of this guide, is and will remain the sole responsibility of the government organisation. This guide serves as a tool for government organisations to – based on general legal frameworks – effectuate this responsibility in a proper and concise manner. The guide thereby wants to contribute to transparency, accessibility and credibility of the government and the legal security of citizens and businesses.

## Version 2

New in this version 2 of the guidebook are the chapters 2, Definition and Context, 5. Authorisations, 6. Application-to-application traffic, 7. Return Flows and 8. Single Sign On. A chapter on the Digital Signature is in preparation. The chapter will be available by the end of 2013.

# Table of Contents

# 1 Introduction

## 1.1 Uniform assurance levels as a prerequisite

The government is investing in large-scale comprehensive electronic government services (e-government services) for citizens and businesses. The coalition agreement defines as one of its objectives to have all government services electronically available by 2017. This way the government wishes to achieve a reduction in the administrative burden, improved provision of services and in general a more efficiently operating government.

The Dutch General Administrative Law Act requires that electronic traffic between citizens and authoritative bodies takes place in a ‘sufficiently reliable and confidential’ manner. In addition, the *Besluit voorschrift informatiebeveiliging rijksdienst* (governmental information policy guidelines) also states that the relevant line management team must determine the assurance requirements according to a risk assessment. Subsequently it must ensure that appropriate measures are taken to meet the assurance requirements. This makes the Dutch General Administrative Law Act *(Awb)* and the *Besluit voorschrift informatiebeveiliging rijksdienst* into open standards, in the sense that their requirements have not been concretely defined.

The on-going surge of the use of e-services has also increased the need to further supplement these open standards. It is important that government organisations in similar situations require (and implement) the same levels of assurance for their e-services. This contributes to the transparency, accessibility and credibility of the government. Furthermore, in the vein of due diligence, it is important that the rationale behind the determination of an assurance level is clear and transparent. This will be in the benefit of the legal security of citizens and businesses. This guide provides this certainty and is based on the nationally valid (legal) rules and is consistent with the European STORK[1] framework for the cross-border use of e-services.

## 1.2 Guide offers sense of security

There is a wide diversity of e-government services. In view of this diversification it is impossible to find a uniform solution for identification, authentication and authorisation. A standard solution with a high assurance level would in many cases be too expensive and therefore unnecessarily impose limits on the use of e-services. A solution with a low assurance level can involve substantial risks regarding fraud and privacy protection. So it seems inevitable that a citizen has to use different solutions for different services.

In order to avoid a proverbial ‘digital keychain nightmare’ for users of these different solutions, the government is currently working towards generically implementable solutions. Examples are DigiD (e-signature), PKIoverheid and

[1] Secure identities across borders linked. See document D2.3 - Quality authenticator scheme, paragraph 2.3 and 2.4, available at www.eid-stork.eu, under ‘STORK Materials > Deliverables - Approved/Public’.

the eHerkenning (eRecognition) appointments registration system. This is also for the sake of managing the costs.

## 1.3 Simplified risk analysis with a classification model

The basic question remains, however, which tool ought to be used in different situations. In practice this has proved difficult to determine for implementers of public services. This guide has been compiled against this background. It is intended to contribute to a concise, efficient and responsible determination of the assurance level of electronic government services. The guide includes a 'classification model' which is in fact a simplified risk analysis. The classification model enables a generic association of (types of) services and assurance levels based on (legal) criteria. The guidebook also includes indications which may lead to classification in a higher or lower assurance level. It does not include an association (mapping) of the assurance levels to specific authentication tools.

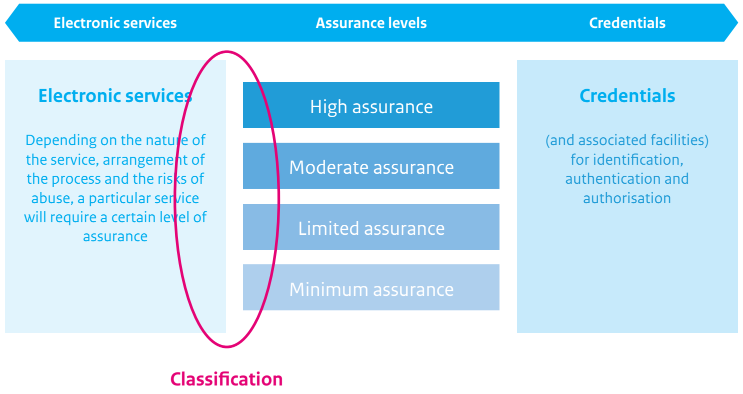

Electronic services
Assurance levels
Credentials
Electronic services
Depending on the nature of the service, arrangement of the process and the risks of abuse, a particular service will require a certain level of assurance
High assurance
Moderate assurance
Limited assurance
Minimum assurance
Credentials
(and associated facilities) for identification, authentication and authorisation
Classification

*Figure 1: Scope of application of the guide*

Using this classification model, architects, information security personnel, lawyers and authorities can make a qualified choice for the appropriate assurance level for the e-services their organisations offer. It is important to realise that this guidebook is based on a generic approach. It will therefore provide an adequate assurance level determination for the majority of cases, but exceptions are possible. If in a certain situation a choice cannot be made using the classification model, e.g. because the nature of the service or the relevant circumstances are considerably different from what is included in the classification model, it will be necessary to conduct a comprehensive risk analysis in order to determine the assurance level for the service.

Furthermore, it is advisable that the service provider makes the classification of their services available in a scheme (policy rules or general binding guidelines, depending on the context). An explanatory note will substantiate the classification so that this is also clear to the users of the service.

## 1.4 Realisation and management of the guide

This booklet was compiled in collaboration between various government organisations and some businesses[2], facilitated by the Standardisation Board and Forum. One of its objectives was to gain an insight in which assurance level is appropriate for different (types of) services. The scope of application for standards describing a specific solution with a specific assurance level is now clearly distinguished.

In the autumn of 2011 the Standardisation Board approved the first version of the guidebook. Following this approval the guide was widely distributed amongst government organisations, accompanied by a recommendation regarding how they may incorporate it into their implementation policies relating to e-services.

This guide is not a static document. On publication of the first version it was clear that the continued development of e-services and of identification and authentication tools, in combination with experiences of government organisations with implementing the guide, will reveal the need for any revisions and additions. Logius and the Standardisation Forum will continue to support the guide's management and further development. This is in line with Logius' management responsibility for various identification and authentication tools and standards, such as *DigiD* (e-signature) and *PKIoverheid*, and *eHerkenning* (eRecognition).

The parties which have been involved in the development of this guide constitute the foundation for a community of users which supports the Standardisation Board and Forum in the maintenance and further development of this guidebook. This second version of the guide is the first substantive addition in which this community has acted as such.

## 1.5 Reading guide

Chapter 2 describes the definition and context of this guide. What is it about, and what is it not about? Chapter 3 contains the initial principles and assumptions for the compilation of the classification model. Chapter 4

[2] Tax Bureau, CoC, *AgentschapNL*, IND, *Dienst Regelingen*, Nictiz, Amsterdam municipality, Ministries of Domestic Affairs, Economic Affairs and of Infrastructure and the Environmment.

elaborates further on the method used and includes the actual classification model for classification of services based on the required assurance level. These three chapters constitute the body of this guide. The chapters 5 to 8 deal with specific forms of communications or service provision. In succession these are: authorisations, application-to-application traffic, return flows and Single Sign Ons. Annex 1 explains the legal framework in which different criteria for the classification of services according to the required assurance level are substantiated. Annex 2 contains several illustrations of the manner in which legal requirements and formulations translate/relate to the actual electronic dimension. Annex 3 includes a list of common terminology.

## 1.6 More information

The guide is digitally available at the websites of Logius and The Standardisation Forum (www.logius.nl, www.forumstandaardisatie.nl) and from the *eHerkenning* ('eRecognition') programme (www.eherkenning.nl). Questions regarding the application of this guide may be directed to: Forumstandaardisatie@logius.nl.

# 2 Definition and context

## 2.1 Definition

### 2.1.1 Types of services

The guide addresses services and processes which the government provides to or implements for the benefit of citizens and businesses. This concerns the domain which is essentially regulated by section 2.3 of the General Administrative Law Act *(Awb)*. In general, the following situations are distinguished:

1. Services whereby an individual uses the service on his/her own behalf via the internet and also completes the necessary steps him/herself (e.g. visit website, send e-mail, etc.). This definition includes both citizens and business.
2. Services which are used by an individual who completes the required steps him/herself, but does so on behalf of another natural person or legal entity (authorisation).
3. Services whereby automated systems communicate with each other without direct human involvement (application-to-application traffic).

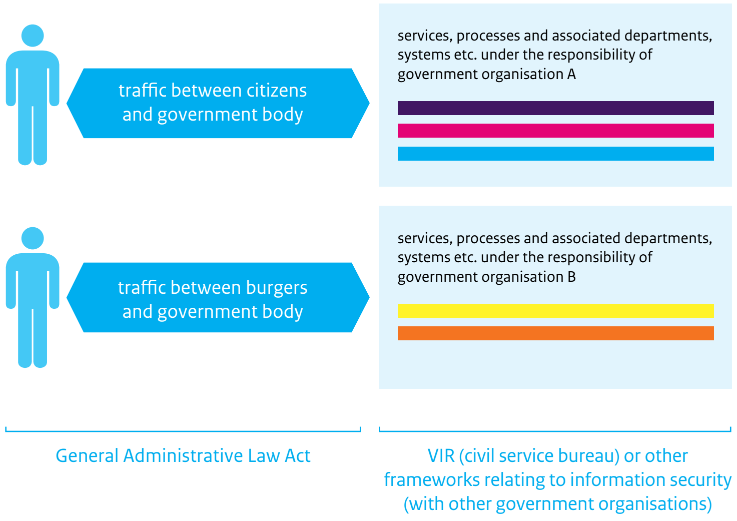
The first version of the guide only addressed situation 1, but this renewed version also describes situations 2 and 3. This guide now also includes the so-called return flows of the service provider to the citizen or the business. First and foremost ‘return flows’ refers to the reaction of the government to an application, registration and suchlike. But even if the first step in the interaction is initiated by the government, such as in official notifications or invitations to register, this will be considered as return flow. Identification, authentication and authorisation play an important role in return flows. It is important that it is understood that the organisation/employee ‘behind the counter’ is authorised to take certain decisions and may have access to relevant information. Confidentiality must similarly be safeguarded in such a case. The same applies to exchanging of data between government organisations amongst each other (e.g. to consult basic (e.g. municipal) registration records, or the exchange of information required for the assessment of an application for a permit).

This domain of ‘return flows’ is (in any case for the ministries and their direct subordinate departments) covered by the *Besluit voorschrift informatiebeveiliging rijksdienst* (VIR, government information security regulations). Decentralised governments typically already voluntarily employ a similar methodology, which means they operate in the vein of the VIR. Additionally, they are – like the various governmental departments – bound to the information security regulations pursuant to the *Wet gemeentelijke basisadministratie persoonsgegevens* (*Wet GBA*, Municipal Personal Records Act) and (the content of) article 13 of the *Wbp* (Dutch Data Protection Act). The administrative organisation and internal control (AO/IC) and the government organisation’s security policy must, based on all these rules, fulfil the required assurances for the reliability and confidentiality of the data streams. See also figure 2.

Finally the subject of Single Sign On (SSO) will be addressed and the specific items requiring attention of the providers of government services. A chapter on the digital signature is in preparation. This chapter will be available by the end of 2013.

### 2.1.2 Assurance level per individual service

This guide aims at the determination of the required assurance level for a particular service. A service provider may offer multiple services requiring different assurance levels – this guide does not specifically state which measures to take in such situations but instead outlines risk-increasing and risk-reducing aspects relating to service provision. This offers valuable reference points in order to restrict – within limits – the number of assurance levels used by an organisation.



traffic between citizens and government body
services, processes and associated departments, systems etc. under the responsibility of government organisation A
traffic between burgers and government body
services, processes and associated departments, systems etc. under the responsibility of government organisation B
General Administrative Law Act
VIR (civil service bureau) or other frameworks relating to information security (with other government organisations)

*Figure 2: Relationship between Awb (General Administrative Law Act) and regulations relating to information security*

[8] Articles 2:13-2:17, included in the *Wet elektronisch bestuurlijk verkeer* (Act on Electronic Government Communications), (Stb. 2004, 214).

## 2.2 Context

### 2.2.1 Trend towards outsourcing and external confidential services

This guide is meant for a service provider offering an individual service and structuring and managing this service themselves. With the intention to reduce the burden of management, costs and risks, government service providers increasingly often outsource all or part of their confidential services.

In the case of partial outsourcing the service provider contracts the structuring and/or management of the confidential services out to a third party, but defines clear requirements. The service provider also needs to be certain they can continue to control the provision of the service.

The second trend visible is that service providers are increasingly using the existing authentication tools and confidential services from the market. A concrete example is the use of social login. People can identify themselves with their Facebook identity and log in with other service providers, such as web shops. The government intends to reduce the administrative burden for citizens and businesses and therefore this is a relevant trend. For using the existing tools or platforms reduces the user's 'digital keychain'. This form of complete outsourcing often allows the service provider no or only limited possibility to determine the exact features of the authentication, authorisations and signature. A kind of 'shake-out' is taking place among the authentication tools in the market at the moment.

Both in case of partial and complete outsourcing the service provider must realise that they will continue to be responsible for the reliability of their own service. This implies they must always ascertain the assurance level of their service themselves, but in addition must be able to make high demands on the third party suppliers and their authentication solutions in terms of reliability and quality. Accountability and supervision need to be well organised. There is no fundamental distinction in this respect if outsourcing takes place to the market or if the organisation makes use of the common facilities of the electronic government, such as DigiD. How this quality and reliability may be safeguarded in outsourcing situations is not included in the scope of this guide.

### 2.2.2 Relying on confidential service certificates

Relying on confidential service certificates enables the service provider to rely on a user of their service being who he claims to be. However, it is not enough to determine the user's identity in the case of many services. We also need to know if the user is authorised, with or without a third-party authorisation, to perform the actions he wishes to perform in the service. And if indeed he has the authorisation, how long it will be valid.

**Example**

Johnson & Johnson Law Firm employs four lawyers. They are assisted by Mrs Smith. This Office Manager takes care of many of the practical issues. She manages the lawyers' schedules and when there is a lawsuit she sees to the logistics of submitting the documents. The lawyers have a lawyers' pass and Mrs Smith has a so-called authorised representative's pass of the Netherlands Bar Association, which she can use to access the court systems on behalf of the lawyers.

Mr Johnson wants to add some documents to the file of a certain case. He signed the documents digitally in the special cloud service identifying him on the basis of his A-number in the Netherlands Bar Association register and issuing a 'certificate of association' which guarantees that Mr Johnson has signed the document. Mrs Smith submits the digitally signed documents electronically through the portal of the court, effectively adding them to the file. Authentication takes place according to her authorised representative's pass of the Netherlands Bar Association. The systems of the court receive Mrs Smith's identity in an identity certificate and the confirmation she is authorised by Mr Johnson for the particular service at the court in an authorisation.

Ascertaining the users' identities and authorisations in electronic services is based on 'Certificates'. Sometimes these certificates will be drawn up by the service provider, but as service providers increasingly obtain confidential services from third parties, these certificates are drawn up by 'outsiders' more and more often, even to such an extent that certificates of different third parties may appear when one single service is used.

Therefore, depending on the complexity of the service and the measure of outsourcing, a service provider may be faced with different types of Certificates. In that case it is important that the service provider can trust the certificates - and the processes they resulted from - are reliable. Simply put: if the provision of the service is classified as assurance level 3, the certificate will have to be of at least the same assurance level. Although this is an essential point (for the reliability of a service is only as good as its weakest link) and in the chapter on 'authorisations' it is further elaborated, the criteria which give a certificate a particular assurance level are part of the standards such as STORK which regulate the 'suppliers' side'. This excludes them from the scope of this guide, which addresses the 'demand side' and therefore answers the question what assurance level a particular service needs.

# 3 Initial principles & assumptions

In this chapter the initial principles and assumptions are described which were adopted for the compilation of this guide. These concern:

- Opting for a simplified and intuitive risk analysis.
- Defining families of services.
- Adoption of the STORK framework as a foundation for interoperability.

The outcome of the approach is a methodology which gives a general estimation of the risks of a specific e-service and which is implementable with relatively little effort. This allows government organisations to determine a required assurance level in a straightforward manner, unless a detailed risk analysis is warranted or mandatory based on rules for information security.

## 3.1 Simplified risk analysis with a classification model

In a number of countries the classification of assurance levels is based on risk analyses[3]. The US has also adopted this approach. The Office of Management and Budget established the E-Authentication Guidance for Federal Agencies in 2006. This guideline states that each body of the federal government must determine the appropriate assurance level for each separate process or service, based on an estimation of the risks in relation to a great number of variables. It is expected that in time, based on the documented risk analyses, certain fixed rules will become distinguishable. This detailed risk analysis for determining assurance levels is inspired by the liability aspects which play a dominant role in Anglo-Saxon culture.

In The Netherlands such an approach would be ineffectual. It is costly, time-consuming and can still lead to fragmentation and unjustified inconsistencies, while processes and services typically show many common (mutual) features (e.g. through the application of the General Administrative Law Act on decision-making processes). That is the reason why a methodology was sought to generically estimate and consolidate risks. This system assumes an estimate of the value at stake, according to a number of objective (or objectifiable) criteria and interests. Examples of this are legal requirements, the nature of the data exchanged (e.g. is personal information involved?) and the economic or social interest associated with a certain service or process.

Subsequently a prediction can be made of the potential damage in case the authentication for the service cannot be performed in the right manner. The assumption implied with this method is that the associated services are provided from within similar online environments and have similar vulnerabilities. The system used does however take into account the fact that

[3] See Spain, for example: MAGERIT, Methodology for Information System Risk Analysis and Management

offline measures can also be taken in order to ensure the confidentiality of data and to reduce the risk of a stolen or forged identity. These measures may include reporting back through another avenue, e.g. a letter to the residential address recorded in municipal personal records.

## 3.2 Families of related services

As mentioned earlier, the processes behind e-government services are often of a similar nature and structure. They generally follow a standard decision-making process, according to the rules of the General Administrative Law Act, possibly supplemented with requirements of domain legislation. Their relative uniformity means that families of related services are definable, even if they differ with respect to the information required for the execution of the service and its (technical) structure (online portal, application).

We distinguish between the following families of related services:
- Requesting general information;
- Signing up for/responding to discussion forums;
- Applying for newsletters etc.;
- Requesting physical government services (waste container, collection of bulky refuse);
- Registration for a personalised web page (a My Domain);
- Submitting complaints;
- Submitting applications (for a decision);
- Requesting/viewing personal information (Cf. pre-completed form);
- Providing/adjusting information;
- Accountability;
- Filing objections;

These families of related services make it possible to make general conclusions about the required degree of reliability for each family. This will be determined by the general and specific characteristics of the particular service. General characteristics include the nature of the data (personal details demand greater certainty than non-personal data). Specific characteristics constitute legal requirements associated with the service (e.g. a (e)signature requirement). This has been an important assumption for the classification of services and assurance levels in this guide.

## 3.3 Stork framework as a basis

Once the assurance level has been established for a particular e-government service, the concrete implementation of the service will be the next step. This includes the choice for the authentication procedure and tool to be applied. The supply of authentication tools is wide and very divers. There are vast differences in user friendliness, price and assurance levels. We are not only considering the Dutch market. There are an increasing number of cross-border services, which must allow access to the Dutch services also with foreign authentication tools.

In order to answer the question of which tool to employ to facilitate the use of a certain service from one country in another country, it is essential to be able to classify the relevant identification and authentication tools. In this context there are several prescriptive documents by now, the STORK framework 6 being the most relevant for the Dutch government. The STORK framework for ‘Quality Authentication Assurance Levels’ 7 was initiated with an eye towards improving the interoperability of electronic identification and authentication in Europe.

In this guide the STORK framework is used as a basis for the definition of assurance levels, so that services and tools may be easily coupled. It must be noted, however, that STORK restricts itself to the authentication of citizens or businesses and even then especially within the context of web portals. For all other matters, such as authorisations, application-to-application traffic and electronic authorisations there are hardly any generally accepted standards available which offer or enable a classification of assurance levels.

## 3.4 The Stork assurance levels

The first step employed in the STORK framework for establishing the assurance level of an authentication tool (credentials) is the assessment of the following independent aspects:
- The quality of the identification (or more precise: identification verification) of the person for registration during the application process for the credentials;
- The quality of the procedure with which the credentials are issued to the user;
- The quality of the organisation issuing the credentials and facilitating the associated registration process;
- The technical type and robustness of the credentials;
- The security features of the authentication mechanism used to recognise the credentials every time it is used remotely (via Internet).

The first 3 aspects serve primarily as procedural safeguards which apply to the registration process. The last two are more technical aspects of the manner in which the credentials are used. The eventual assurance level of the authentication tool is determined through a combination of these aspects. The STORK framework assumes 4 levels. The individual aspect with the relatively lowest score (the weakest link) will ultimately determine the applicable assurance level. This is illustrated in the figure on the next page.

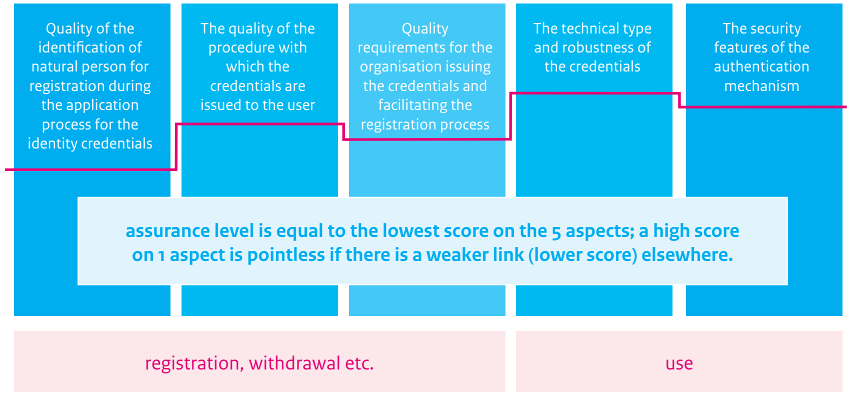

Quality of the identification of natural person for registration during the application process for the identity credentials
The quality of the procedure with which the credentials are issued to the user
Quality requirements for the organisation issuing the credentials and facilitating the registration process
The technical type and robustness of the credentials
The security features of the authentication mechanism
assurance level is equal to the lowest score on the 5 aspects; a high score on 1 aspect is pointless if there is a weaker link (lower score) elsewhere.
registration, withdrawal etc.
use

*Figure 3: Determination of the assurance level according to STORK*

The 4 levels defined by STORK are:

*STORK QAA level 1*
This is the lowest assurance level; it either assures a minimal confidence in the asserted identity of the user or no confidence at all. Identity credentials are accepted without any form of verification. An example of this is a procedure in which the applicant receives an e-mail from the issuing agency with a hyperlink which must be clicked to be able to use the credentials. The only certainty is that a similar email address exists at the time of application and that an unidentified applicant would be able to respond to e-mail messages sent to that address. An example of this is downloading of a tender document from *Aanbestedingskalender.nl*.

*STORK QAA level 2*
At this level, verification of the identity claimed by the user during the registration process for obtaining the authentication credentials takes place. This is done by means of a check based on an official document issued by the State (e.g. a copy of the user's passport or driver's licence) or registration (e.g. in the Municipal Personal Records). Claimants are not required to appear physically during the registration process, credentials with a single-factor authentication will suffice. 'Factor' is understood to mean an identity token for a claimed identity, e.g. a user name and password combination or a unique code submitted by a trusted party. Logging in with *DigiD*, for example for declaring one's taxes digitally, employs this method. DigiD is an example of such credentials with a single factor authentication.

*STORK QAA level 3*
This level requires stricter methods for verifying the attested identity of the user. These methods must offer a high level of certainty in identifying the claimant. Identity providers are supervised by the government. A 2-factor authentication is required. Examples would be soft certificates or one-time password tokens. The Dutch Road Transport Directorate (RDW), for example, uses the 2-factor authentication in its communication with businesses in the vehicle sector which is authorised in that capacity to view certain RDW data. Online banking applications for which customers need a token also employ this level of authentication.

*STORK QAA level 4*
This level requires at least the one-time (for initial registration) physical presence of the user for the registration process and compliance with all requirements of national law of the relevant country during issuance of qualified certificates as intended in Annex II of the e-signature Directive 1999/93/EC. For The Netherlands this concerns the requirements of Article 1.1, part ss, of the Telecommunications Law. The identity credentials provider must furthermore fulfil Annex I of the same directive. In The Netherlands this article is addressed in article 18:16, section 1, of the Telecommunications Law. Government parties or for example notaries who wish to submit documents digitally to the national register, can do so through a special application 'Web-Elan'. This system requires the use of a token, an authenticated certificate and a digital signature. Users must ensure these themselves.

# 4 Mapping of services

Pursuant to the initial principles and assumptions of chapter 3 a classification model has been formulated for the classification of e-government services at various assurance levels. This classification model essentially serves as a simple risk analysis. The required assurance level for a certain service can be estimated based on a number of criteria. These criteria all concern the legal requirements of the service, the nature of the data and the potential damage if they were to be obtained or modified by unauthorised third parties.

The method used, which is related to the usual elements of risk analysis, the threat or the chance that a threat will manifest itself is not quantified. Instead, assumptions are formulated with respect to the quality of the IT security features and other relevant features of the background processes through which the particular service is provided. These assumptions are incorporated into a so-called reference scenario. Based on the criteria and this reference scenario, an assurance level can subsequently be assigned by consulting a simple table (the 'classification model', see page 31).

The classification model also has a number of correction factors. These factors reduce or increase the threat in relation to the reference scenario. Especially in the latter case, such a simple risk analysis will not suffice and a comprehensive risk analysis is still called for.

## 4.1 Criteria

The following criteria relate to the mapping of assurance levels:

**1 Legal consequences**
If a particular service is based on legislation, this will lead to legal actions by the government organisation (e.g. taking a decision subject to appeal) and will as such be aimed at legal consequences. For cases involving actual performance (e.g. provision of information) the service will not imply legal consequences. It may happen that a certain service initially purely involves actual performance, but that ultimately it still leads to legal consequences. An example of this is the registration of municipal waste containers according to name and address, whereby these details can also serve as a basis for implementation (e.g. for the correct scheduling of waste collection). This is important for the classification of the assurance level.

Applicable values:
- No legal consequences;
- Legal consequences;
- indirect legal consequences.

**2 Formal legal requirements**

Many services require a signature, either based on the General Administrative Law Act (Awb) or based on specific legal rules. This may involve signing for the sake of authentication, or to confirm an indication of intent. In specific cases an advanced or qualified electronic signature may even be explicitly required, depending on the level of validation required.

Applicable values:

- Only general requirements relating to reliability and confidentiality are set;
- Signature by or on behalf of the claimant is required;
- Signature is required; other formal requirements also apply to the signature.

**3 Provision of personal information by the individual**

Processing personal information requires adequate security, as laid down in Article 13 of the Personal Data Protection Act (*Wbp*). Naturally this requires a broad range of security measures, of which authentication 'at the gate' is not the only security element, but certainly a very important one, because:

- it prevents the sensitive personal information to fall into the hands of wrong parties or persons;
- provision of (changes to) personal data is always strictly linked to the (reliable) identity of the acting individual.

In this guide the two situations have been separated. On the one hand the situation that the individual provides his own personal data (this paragraph) and on the other hand the situation that service providers communicate personal data already known (see the next paragraph). The reason for this is that if an applicant independently (on his own behalf) provides information, unauthorised information to third parties of course cannot occur. But when provided by the government, e.g. by displaying data on a governmental website, this may be the case. That is why the assurance levels in these two situations are classified differently.

The criteria for mapping the sensitivity of the personal data are primarily the nature of the personal data and secondarily the nature of the processing [Dutch DPA Guidelines for the Protection of Personal Data, 2013].

The DPA guidelines mentioned therefore provide a very open standard, but this guide seeks to provide a classification inspired by the former DPA publication A&V 23.8. For the classification we will only adopt the 'nature of the data' criterion, however. This classification into categories has been chosen because the open approach of the guideline proved not enough to go by in practice.

| Category | Nature of the information |
|---|---|
| No personal information | The information cannot be traced back to an identified or identifiable person. |
| Risk category 0 | Public information.<br>Publicly available personal information which has been generally acknowledged to not form a risk for the involved individual. Examples of this are telephone books, brochures and public internet websites. |
| Risk category I | Basic information.<br>Limited number of personal details relating to a single type of validation, e.g. membership, employment or client relations, provided that these cannot be considered to be special personal data. |
| Risk category II | Increased risk.<br>Special personal data as intended in article 16 of the General Administrative Law Act (*Wbp*), or financial/economic information relating to the involved individual. |
| Risk category III | High risk.<br>Data collected from investigation authorities, DNA database, information subject to special legal confidentiality obligations, information falling under a code of professional secrecy (e.g. medical) as intended in article 9, part 4 of the General Administrative Law Act (*Wbp*). |

The nature of the processing is incorporated in the classification into the following categories: "Processing of personal data", as intended in Article 1, part b of the General Administrative Law Act (Wbp), is understood to mean: "every action or every sum of actions relating to personal data [...]". This therefore concerns all data processing ranging from collection to destruction. The nature of the processing may in fact be an aggravating element. One should be thinking of a large quantity of an individual's personal data or an above-average major impact the loss or unlawful processing might have. The risk and damage for the individual are always at the centre. To put it extremely, it is therefore irrelevant if the data of a few or millions of persons are processed.

Applicable values:

- There is no processing of personal data, or the data cannot be traced back to identified or identifiable persons.
  Publicly available personal information which has been generally acknowledged to not form a risk for the involved individual. Examples of this are telephone books, brochures and public internet websites.
- Category I (Basis);
  Limited number of personal details relating to a single type of validation,

e.g. membership, employment or client relations, provided that these cannot be considered to be special personal data.
- Category II (Increased risk)
  Special personal data as intended in Article 16 of the General Administrative Law Act (*Wbp*), or financial/economic information relating to the involved individual.
- Category III (High risk)
  Data collected from investigation authorities, DNA database, information subject to special legal confidentiality requirements, information falling under a code of professional secrecy (e.g. medical) as intended in Article 9, part 4 of the General Administrative Law Act (*Wbp*).

The categories of personal data are designated as follows:

***Step 1.*** Make an initial prediction of the category based on the nature of the data, according to the table above.

***Step 2.*** Determine any aggravating factors. The nature of processing plays an important role in this. The first aggravating factor may be the processing of a large quantity of data per individual (multiple validations, multiple purposes). The second aggravating factor may be the processing of multiple data of multiple persons. A third aggravating factor may be, if the purpose of processing can lead to an above-average major impact in case of unlawful processing or loss of personal data.

***Step 3.*** If one or more aggravating factors exist, advance to the next risk category (one category up). An exception to this is financial/economic information, which is not subject to aggravating factors. This information is always classified as category II.

### 4 Displaying personal data, other than that provided by the user in the same session

With electronic services it may occur that personal data is provided or shown through a website or in a message by the service provider to a citizen or business. This personal data may also be exchanged between applications. Because unauthorised validation may occur here, as a rule a higher assurance level is required than for the provision of the same (type of ) personal data by the involved individual. That is why the displaying of personal data by a governmental website (or the provision of this data in a message) will receive a higher sensitivity designation with respect to mapping: a higher assurance level is required for information within the same risk category. See the adjoining table for further explanation about the applicable categories.

Applicable values:
- No personal data in addition to the information independently provided;
- Category 0
- Category I
- Category II
- Category III

### 5 Processing of the BSN Number

Following on the criteria with respect to the processing/recording of personal data, the recording of the BSN number (Citizen Service Number) is applied as a separate criterion. The BSN number is by definition a key which can simplify the coupling (aggregation) of personal data, both within and amongst organisations. Moreover, stringent legal requirements apply to the use of BSN numbers.

Applicable values:
- BSN not recorded
- The BSN number is exclusively provided by the user and potentially mapped (possibly in combination with for example a name for the sake of certainty about the correctness of the BSN number provided);
  The implicit provision of the BSN number by *DigiD* use is included in this;
- The BSN and any supplemental personal data not provided earlier in the process are displayed.

### 6 Correctness of the provided information

A special category is formed by the recording of the data provided in a basic registry. After all, the potential consequences of inclusion of information in such a register can be considerable, since users of the basic registry are obliged to use the information from the registry. A distinction is made however with respect to mutations in non-authentic data and mutations in authentic data, for the obligatory use only applies to the authentic data.

Applicable values:
- There is no mutation or creation of a basic registry based on the data provided;
- Mutations of non-authentic data in basic registers;
- Mutations of authentic data in basic registers;
- Creation of authentic data in basic registers

### 7 Economic interests

Invalid identification may affect economic interests and lead to economic damages. This may involve financial damages due to misuse (abuse) or fraud, access by unauthorised parties to competition-sensitive information (potential lost order severity) or leaking of market price-sensitive information.

| Criteria | Assurance level |
|---|---|
| - no legal consequences<br>- general requirements set for reliability and confidentiality<br>- provision by involved individual (independently) of public personal data (risk category 0)<br>- no displaying of personal data by governmental service provider<br>- BSN Number not recorded<br>- no mutations in basic registry<br>- economic interest: zero<br>- public interest: low | 0 (no authentication requirements) |
| - no legal consequences<br>- general requirements set for reliability and confidentiality<br>- provision of personal data, up to and including risk category I<br>- displaying of personal data, up to and including risk category 0<br>- BSN Number not recorded<br>- no mutations in basic registry<br>- economic interest: zero<br>- public interest: low | 1 |
| - possible legal consequences<br>- legal requirements with respect to signature<br>- provision of personal data, up to and including risk category II<br>- displaying of personal data, up to and including risk category I<br>- BSN Number is recorded, provided by user, possibly using *DigiD*<br>- no mutations in basic registry<br>- economic interest: limited<br>- public interest: medium | 2 |
| - legal consequences<br>- legal requirements with respect to signature or desired action<br>- provision of personal data, up to and including risk category III<br>- displaying of personal data, up to and including risk category II<br>- BSN Number is recorded, whether or not provided by the user<br>- mutation of non-authentic data in basic registries<br>- economic interest: average<br>- public interest: medium | 3 |
| - legal consequences<br>- legal requirements for signature, other formal requirements<br>- processing of personal data of risk category III<br>- displaying of personal data - risk category III<br>- BSN Number is recorded, whether or not provided by the user<br>- processing of data leads to mutation or creation of authentic data in basic registry<br>- economic interest: great<br>- public interest: high | 4 |

Applicable values:

- Zero: There is no economic value – at least no economic damages – to be expected in the event of invalid/incorrect identification/authentication;
- Limited: This concerns only limited economic interests of the individual; Incorrect identification/authentication can lead to damages in the order of €1,000;
- Average: This involves greater interests at the individual level or limited business interests. Potential damages are absorbable and/or rectifiable. Involves amounts up to the order of €10,000 per case;
- Significant: Economic-scale damages (significantly) more than €10,000.

**8 Public interests**

In the above the interests of the individual citizen or the individual business was put at the centre, but this concerns the common interests. We can distinguish public, political and social disruption.

Applicable values:

- Public – disruption of public trust in service provision
  Low: Complaints, commentary in newspapers;
  Medium: Ombudsman intervenes, official parliamentary questions, etc.;
  High: Minister resigns.
- Social disruption
  Low: Disruptions which can be resolved with a single organisation's resources;
  Medium: Disruptions demanding coordinated efforts by multiple organisations, mostly public and private organisations;
  High: Urgent situation; disruptions requiring emergency measures not accounted for in the normal legal, financial (etc.) framework

## 4.2 The classification model

In the classification model on the previous page the defined criteria are mapped against the assurance levels. By designating the most appropriate values to each of the 8 criteria for the corresponding service, the appropriate assurance level can be determined.

## 4.3 Reference scenario

The classification model is very useful for an average process or IT vulnerability. The assumptions about this average vulnerability are explicitly stated below, and essentially constitute the reference scenario. A number of common deviations/inconsistencies with respect to this scenario have been identified as correction factors; that is, these factors (may) lead to an adjustment of the assurance level determined based on the classification model or to the conclusion that a full risk analysis must be executed.

Assumptions relating to distinguishing the type of service and its users:
- This concerns interactive, online services for citizens and/or businesses and besides application-to-application traffic and return flows;
- Citizens independently (on their own behalf ) use services, or have authorised representatives use services for them. Employees use services on behalf of the company they work for;
- The type of scheme and corresponding type of service process involved are clearly distinguished.

Assumptions relating to the control of IT security and privacy:
- The organisation has working management systems for information security and protection of personal data;
- An implemented and current security plan is in place for IT for the particular service in question. This plan is based on common standards and/or a specific risk analysis;
- It is (made) known which personal data is processed for the specific scheme/ service as well as the manner in which these are processed.

Assumptions relating to the process which facilitates the service/scheme:
- The valid legal requirements for the service are complied with;
- The user's identity is authenticated when providing access to the requested service. This identity is subsequently adopted in the system during for following process;
- Supplemental measures for verifying this identity via alternative avenues remain restricted to back-office controls; there are no extra controls whereby the user is asked to provide additional validations with respect to their identity;
- For services involving a decision by an authoritative body, the decision will always be communicated to the concerned person. Other involved parties may also be notified. This may take place via another avenue than through which the service was originally requested.

## 4.4 Correction factors

The assumptions outlined above (the reference scenario) and the classification model based on these assumptions will not provide a correct outcome for all situations. Both risk-increasing and risk-reducing factors exist.

Risk-reducing factors mostly occur when there are extra steps in the process mitigating the risk. Based on this a substantiated argument can be made for a lower assurance level than the classification model proposes.

Risk-increasing factors relate mostly to the context of the service in question. These involve factors such as political or managerial sensitivity and/or the effect on image (reputation). In this guidebook the choice is made not to be restricted to the prescription of a higher assurance level, but to recommend a full risk analysis in such cases.

**Risk-reducing factors**

1. In the subsequent process a step is included in which the party involved must appear physically and identify himself (ID document and BSN number). This is to safeguard that the party involved does indeed want to use the service in question with the data in question provided.
2. Feedback with respect to mutations or (proposed) decisions takes place via another avenue than the original (electronic) channel.
3. In the subsequent process there is a step which includes data or documents evidencing the involvement and consent of the person involved, apart from the use of the service.
4. There is a continuous and active monitoring which prevents a service from being accessed excessively by the same individual in a short space of time, or for preventing other usage behaviour which may suggest fraud. Keeping risk and maintenance profiles can be ranked among these.
5. When the economic interest is the determining factor in establishing the assurance level and when financial services are concerned: verification of the bank account details for the account into which payments are deposited.

If a risk-reducing factor applies, then the reduction of the ultimate assurance level may be possible in a single step. However, in cases where legal requirements determine the assurance level (e.g. formal signature requirements), reduction will not be possible.

Reduction from assurance level I down to 0 is also not permitted; Risk-reducing factors can never alter the nature of the data. In case of personal data measures will always be necessary to warrant the reliability and confidentiality of these data.

**Risk-increasing factors**

Situations which warrant a comprehensive risk analysis:
- The service is subject to an inherently political, managerial and image (reputational) risks;
- The risk is difficult to determine since only a limited degree of damages attributable directly to the incident is possible, even though significant consequential damages are possible (different from the situation in which a mutation takes place on authentic data in basic registries);
- The service involves a high potential for large-scale abuse. Especially the combination of sizeable processes, limited verification possibilities and, at a large scale, major potential profits.

## 4.5 Examples of services and corresponding assurance levels

By way of example, this section refers to different services and their corresponding assurance levels according to the criteria above.

| Criteria | Assurance level |
|---|---|
| Anonymously visiting government websites | 0 (no requirements) |
| Municipal local services (e.g. reporting deficiencies in public areas, requesting waste containers) | 1 |
| Registering for personalised portals (MijnOverheid.nl, mijndenhaag.nl, etc.)<br>Municipal permits (tree pruning/cutting permits, event permits, etc.)<br>Environmental permit for private individuals<br>Financial benefits eligibility for private individuals (subsidy, unemployment benefits, other allowances)<br>Au pair residency permit<br>(Status) information in *MijnOverheid.nl*<br>Reporting/registering<br>Pressing charges (misdemeanours, minor)<br>Reporting changes<br>Tax declarations for private individuals, with no pre-completed information about personal financial situation<br>Fulfilling permit requirements for private individuals<br>Requesting WOZ (immovable property) value | 2 |
| Tax declarations for private individuals; collecting or editing partially pre-completed declaration form (displaying personal data risk category 2)<br>Tender documents<br>Environmental permit for businesses, residency permits for labour/knowledge migrants, official documents (certificate of good conduct, passport, driver's license, etc.)<br>Tax declarations for businesses<br>Financial eligibility for businesses (subsidy)<br>Compliance with requirements for businesses (annual statement, etc.) | 3 |
| Declaration (birth)<br>Consulting medical dossier<br>Pressing charges (criminal offences, serious)<br>Patent applications | 4 |

# 5 Authorisations

## 5.1 What is it really about?

In many situations citizens or businesses are represented by somebody else. Fiscal service providers or a neighbours file the tax returns for citizens. Specialised offices apply for a subsidy on behalf of their clients.

The government is developing an increasing number of e-services. That is why the importance of recognising and supporting authorisations has also increased. For it is not desirable that intermediaries and other representatives ask citizens and businesses for their credentials and use them to sign on as if they were that citizen or business. In other situations the intermediaries themselves claim to represent a specific business or citizen, but the service provider is unable to verify the claim in a simple manner.

To better regulate situations of authorisation in the electronic world, it is important to aim at an authorisation explicitly laid down. Mostly the authorisation is laid down in an authorisation register, which is the foundation for a confidential service. The authorisation register provides authorisation declarations: electronic messages about the authority of the acting party and the certainty of that authority, as well as any details with regard to the authorisation.

## 5.2 The individual service perspective

In principle an authorisation does not affect the assurance level required by the service provider for an individual service; the nature of the service is not affected.

Assuming the authorisations are not kept in the own records of the service provider, special authorisation services are required to register the authorisations and to issue authorisation certificates of an adequate assurance level. If the service requires an assurance level 3, the authorisation certificates will also have to comply with at least an assurance level 3.

This has consequences for the manner of registration and management of the authorisation by the authorisation registers, for they have to be adequately organised to assure the required assurance level. No internationally accepted standards are available for this as yet, but at a European (STORK) and a national (eID scheme NL) level documents with regard to this field are in preparation. Furthermore eRecognition applies standards for assurance levels and authorisations much in line with the concept of STORK. In the documents referred to provisions are set out on the term of validity for authorisations, retention periods and validity of the authorisation certificates.

It is important to recognise authorisations are issued in a chain of which not all steps are necessarily digital. In all cases the holder of the authorisation register will see to the conversion to a digital authorisation certificate. However, it is also conceivable that the authorisation register and its services are not used and that the service provider receives authorisations in a paper, unstructured digital (pdf ) or structured digital (authenticated message) form.

## 5.3 What does this mean for the application of the classification model?

The assurance level ensuing from the application of the classification model applies to the implementation of individual services. Whether or not there is a representation/authorisation, does not affect the criteria or application of the methodology, and therefore will not affect the outcome. For the service provider it is important that the received authentication is of the right level and, in case of an authorised representative, is accompanied by an authorisation certificate at the same assurance level. Whether or not an authorisation is issued is only a matter for the user of the service.

## 5.4 Other items for consideration

In principle the risk of fraud increases with opening up the possibilities of representation. After all, fraudsters may try to claim or register fraudulent authorisations. This risk must be overcome, in the first place by demanding an authorisation each time a service is used, in the second place by formulating sufficiently strict demands on registration and the use of authorisations by way of a reference to prescriptive documents in this area (of eRecognition, or later the eID scheme NL or European guidelines).

If registration of an authorisation constitutes a substantially higher barrier than the use of the service, undesirable behaviour, such as passing on of credentials to intermediaries, as presently occurs, will continue to pose a problem. This should be taken into consideration when authorisation plays a role in a service offered. The service provider could also consider to report the authorisations and in this case the use of the authorisations back to the parties involved. The citizen or business involved thus gains a clear insight into which party uses government services on his or its behalf.

# 6 Application-to-application traffic

## 6.1 What is it really about?

Human intervention is becoming increasingly rare in electronic services. If a computerised entity's service is used by another computerised entity this is called application-to-application traffic. A distinction is made between 'channel' and 'contents' for the security of this traffic.

- Channel security.
  By securing the channel a 'safe tunnel' is created between the organisation supplying the service and the organisation using the service. Both sides know where the tunnel leads to. The tunnel itself secures a safe data transmission. The data cannot be read or changed by a third party;
- Contents security.
  In addition, it is also possible to secure the message itself. A message is then signed or authenticated and possibly encrypted. These messages can be transmitted with end-to-end security. The messages cannot be read or changed during transmission.

Table 1 displays some characteristic differences between channel and contents security.

| Channel security | Contents security |
|---|---|
| **Universal**<br>Different types, contents, often of more applications are possible over the same channel | **Specific**<br>Each type of contents has its own security |
| **Casual**<br>The contents do not show that they have been safely transported | **Lasting evidence**<br>Characteristics proving the authentication are associated to the contents |
| **Secure until first interim stage**<br>Traffic is protected from tunnel entry to where the tunnel 'surfaces' again | **End-to-end security**<br>Safe traffic with chain parties before and behind are possible |

*Table 1: Characteristic differences between channel and contents security*

For both the channel and the contents security the digital certificates constitute in fact the assurance standard. (Similar) digital certificates are required for both types of security, which is why both types are often jointly employed. Previously shared secrets between the parties (such as passwords) are also used to secure, but digital certificates are preferred by far as they provide more security.

## 6.2 The individual service perspective

The following features are characteristic of application-to-application traffic:

- There is no human intervention;
- This concerns communicating applications, the natural person has disappeared;
- Often this concerns bulk data.

> One of the applications for which digital certificates are now implemented is the reliable supply of data within the scope of SBR (Standard Business Reporting). Business or intermediaries about to file their corporation or income tax returns, secure their communications (application-to-application traffic) with 'DigiPoort' with eHelp of a PKIoverheid (services) server certificate. In the years to come many more applications are going to use SBR, such as filing turnover tax returns, filing of the annual accounts and statistical reports.

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

For application-to-application traffic and consequently for the identification of communicating organisations the risk-oriented approach of this guidebook is found not to be very useful. The practice turns out to be about digital certificates, which has in fact reduced the options to a choice of how reliable the certificates need to be. In fact the choice has been made for *PKIoverheid* certificates. This applies to both the channel and the contents security. The BIR standardises on *PKIoverheid* certificates for the reliable authentication of and communication with organisations. Otherwise, for very sensitive application-to-application communications the government propagates the use of a 'private root'.

## 6.4 Other items for consideration

**Lessons from the Diginotar incident**

The Diginotar incident has made it clear that (government) organisations depend heavily on the use of digital certificates for both channel and contents security. Reports such as from the Dutch Safety Board and the Advisory Committee A3 Legal Entities pursue this in greater depth. The three major points the service providers should consider are:

- See to it that for time-critical applications there are backup certificates of alternative certificate service providers available;
- See to it that in your organisation there is more than one certificate manager, i.e. a person authorised to apply for new certificates with various certificate providers on behalf of your organisation, to revoke old certificates etc.;
- Avoid single-points-of-failure, which can result in the entire process coming to halt in case of failure.

# 7 Return flows

## 7.1 What are we really talking about?

The further development of e-government does not only imply that users approach the service provider digitally, but also that the service provider approaches the user or responds digitally. This assumption not only applies to communication with persons but also to interaction between applications. This 'return flow' constitutes an important part of electronic communication.

In practice we distinguish for return flows the following scenarios:

- The 'e-mail scenario'
  The service provider sends an electronic message to the e-mail address of a natural person;
- The 'access to a Web portal' or 'Message Box' scenario
  The service provider places messages on their own, secured web portal and alerts the citizen (through SMS or e-mail) that there is a message for him. The 'Message Box' scenario is a functional, similar version, which makes use of a communal facility: the Message Box. In this scenario the service provider drops the message in the Message Box (for citizens or businesses) instead of at their own web portal;
- The 'application-to-application traffic' scenario
  Through application-to-application traffic the service provider has the return flows transmitted directly to the organisation involved or to the intermediary.

## 7.2 The individual service perspective

It is important that the service provider regulates the following matters in case of return messages:

- The message or document must reach the addressee;
- Unauthorised third parties must not be able to gain access to the message or document;
- The addressee must be able to verify that the message or documents actually originates from the service provider in question.

The above-mentioned matters arise directly from the provisions of the General Administrative Law Act (*Awb*) on electronic traffic. In the case of a return message there is a shared responsibility between the service provider and the addressee to see to it that the return message actually reaches the addressee. The service provider must organise a reliable and safe medium and the citizen or the business must check his or its own mail.
The General Administrative Law Act (*Awb*) leaves it to the citizen or business to open the electronic pathway or not. From the moment they have opened the electronic pathway, they are supposed to be reachable through it.

With this at the back of our minds, this means the following for the scenarios mentioned above:

**The e-mail scenario**
The weakest link in the e-mail scenario is the maintenance of an up-to-date e-mail address by the citizen or business. Citizens and businesses experience but a weak incentive to update their previously provided e-mail addresses. In many respects, moreover, e-mail is a less reliable and confidential medium. Sensitive information must therefore be encrypted. For this the service provider must have a digital certificate of the citizen or business at their disposal. This leads to a problem similar to the problem with e-mail addresses: citizens and businesses do not experience an incentive to make an up-dated certificate available. Also in the case of e-mail, supplementary measures are needed to offer the addressee the opportunity to verify if the message indeed originates from the government. One of the possibilities is authenticating the messages (see the text box 'authentication by the government' under 7.4).

This makes e-mail unfit as a generally applicable medium for the implementation of return flows. E-mail is reasonably fit for reporting back less sensitive information if the citizen or business has shortly before provided the e-mail address to be used. Examples would be general information of service messages.

**The 'Web portal' or 'Message Box' scenario**
Service providers can place return messages on their own web portals and allow citizens access with, for example, DigiD. However, they increasingly use the generic Message Box facility (part of MyGovernment [*MijnOverheid*]) instead of their own web portals. In the Message Box the addressees can open and read any (return) messages from the government in a safe environment. The Message Box sends an alert when new messages have arrived. There is also a Message Box available for businesses, where their return messages can be sent to.

Assuming that the environment of the Message Box (and/or the web portal itself) is sufficiently protected, it is still important to make sure the right person has access to the messages. The Message Box offers these validations to citizens up to assurance level 2 by permitting access with DigiD and by restricting access to a person's messages by means of obtained BSN numbers. An addressee can be quite certain that a document originates from the government, as the source is the Message Box or another reliable web service. This scenario also depends ultimately on the availability of a current e-mail address or mobile telephone number to alert the citizen or the business to a new message. This weakness is a little less prominent than in the e-mail scenario, but it still exists.

**The 'application-to-application traffic' scenario**
In case the service provider sends a return message directly to the organisation concerned, the channel security will see to the desired validations. The channel security secures that no unauthorised third party can gain access to the message, after all. And given the structural character of the implementation of the application-to-application coupling, the reachability of the addressee is well regulated. Therefore an application-to-application coupling is very reliable.

In the case of representation the service provider will want to alert both the intermediary and the party involved. In some special situations intermediaries also supply electronic services to the customers they represent. Therefore it may be considered to have the return flows to the citizen or the business pass through the electronic channel of their intermediary. However, in any case it is the individual who needs to indicate how he wishes to be reached.

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

In principle the classification model applies to access the return message as a service. In practice this means however that the classification model applies to the entire service the return message is a part of. The classification model is devised to designate the data category, so here the data included in the return message are specifically assessed.

The classification produces a desirable assurance level for the return message in the context of the service. Based on the outcome of the classification, the following possibilities are open:

- The e-mail scenario cannot be used for messages with an assurance level higher than 1;
- In the 'Access to a Web portal' or 'Message Box' scenario the authentication assurance level for access to the portal or the Message Box determines to which return messages access can be given. The authentication assurance level for access to the portal or the Message Box must be equal to or higher than the desirable assurance level for return messages that access has been given to;
- In the 'application-to-application traffic' scenario the need for security is sufficiently covered by the PKIoverheid (services) server certificates mostly used for channel security. If the situation is complicated because the ultimate destination of a return message is different from the destination of the application-to-application coupling, a more comprehensive risk analysis will be necessary.

## 7.4 Other items for consideration

**Shifts with legal implications**
We have noticed that the classical model of 'the government sends important legal documents to the recipient', with the associated 'duty to deliver' is slowly being replaced by a model in which the citizen or business has a 'duty to receive'. In fact a certain action will always be required of both the sender and the recipient: to deliver and to receive. The meaning of 'delivery and receipt' may shift according to the technical implementation. Today 'receipt' may be understood to mean that any citizen is required to open and attend to his mail. Tomorrow 'receipt' may be understood to mean that a citizen is required to log on to the government mailbox system or to another service in the 'cloud'.

A second shift concerns the present coordinated character of e-government services to a preferred character. This will affect the legal situation with regard to the return flow as well, although at the moment it is unclear exactly how. At present the General Administrative Law Act [*Awb*] / Act on Electronic Government Communications [*Wet elektronisch bestuurlijk verkeer*] mention coordination of the electronic and paper channel. Citizen and government (government body) deliberately open the channels to facilitate electronic communication. The shift toward 'digitally, unless....', however, is unmistakable and implies that it will become increasingly difficult to avoid a digital form of service provision.

**Authentication of documents by the government**
Often a citizen or business wishes to be able to verify whether certain documents are indeed originating from the public authorities, for example the government. For example in the case of digital documents that need to be submitted elsewhere as evidence. This may concern a wide variety of documents, such as Decisions, Extracts, Official Certificates of a medical or financial situation, etc. Or for example in the case of public announcements, when one wants to be able to establish with certainty that these are official documents issued by a certain government body.

To increase the legal certainty of citizens and businesses it is advisable to authenticate all these types of documents digitally. This authentication can be realised with a digital signature of the government organisation in question.

In this case it must be an authentication on behalf of an (authorised system of an) organisation rather than an electronic signature of an officer of that organisation.

For the sake of interoperability with systems already executing this for documents drafted under the terms of the Services Directive, it is recommended to use the standard formats Pades, Xades or Cades, as set out in Decision EU 2011/130.

Besides the authentication of such documents, a service provider would be well advised to offer facilities to verify authenticated documents online. In cases subject to the Services Directive and using a different format than mentioned above, such verification service is even obligatory.

# 8 Single Sign On

## 8.1 What is it really about?

Single Sign On (SSO) is understood to mean the user's possibility to access various services through a single authentication facility. A user will then only need to sign on with the first service; there is no need to confirm his identity time and again after that. SSO is possible for a body of services of one organisation or domain, but also amongst organisations and domains.

**For example**
When a citizen signs on, MyGovernment [*MijnOverheid*] gives access to a range of (compound) data and services of several (government) organisations, such as the Municipal Personal Records, the Dutch Road Transport Directorate and the Dutch Pension Register [*stichting Pensioenregister*]. After registration, the regulations service portal [*DR-loket*] of the Ministry of Economic Affairs gives access with a single authentication to any number of specific services in the business domain, such as manure registration, numerous subsidies and various regulations on fishery.

An important concept with Single Sign On is the federation. The federation is in fact the group of organisations jointly using an SSO solution. By participation in a federation an organisation expresses their confidence with an added proviso in the authentication coming from the sign-on process (possibly) performed elsewhere with another member of the group.

There are different types of federations. There are federations that authenticate at one assurance level, but there are also federations that facilitate different assurance levels. In the latter case, if the user switches from one service to another with higher assurance requirements than the one he was first authenticated for, he will have to be authenticated again or supplement his authentication. The size of federations may differ widely, ranging from an individual organisation offering a number of electronic services within one portal to a government-wide portal disclosing the services of a large number of different organisations.

Closely related to Single Sign On is Sing Sign Off, where the user terminates the various service sessions at once.

## 8.2 The single-service perspective

From the single-service perspective a Single Sign On is one of the ways to offer an identity and an identity authentication to a service provider. For the service provider it is only important at which assurance level authentication has taken place and if it is still valid.

However, Single Sign On presents a number of questions with a wider scope than just the rationale behind a single service for a service provider. That is the reason why some items for consideration have been named in paragraph 8.4.

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

Single Sign On and the single-service perspective do not shed any new light on the criteria and rationale behind the classification model. Single Sign On is in fact part of the supply of authentication services.

The single service is valued in conformity with the classification model and classified at a certain assurance level. The authentication that gives access to this service must be fit for this assurance level, irrespective of the origin of this authentication.

## 8.4 Other items for consideration

The single-service perspective simplifies thinking about Single Sign On. If the subject is considered in a broader perspective, SSO however has a number of points of special interest which are of importance to service providers. The two most prominent points of interest will be introduced in this guide.

### 8.4.1 Participation in a federation

The service provider should consider whether or not to use authentications emanating from a federation. Several aspects may play a role:

1. The service provider's influence on the implementation and operation of the federation;
2. The possible upward pressure on the assurance level as a result of joining the federation;

There are different types of federations. Some federations have the possibility to support various assurance levels, while others do not. The service provider may find that, if the federation has only one assurance level, this may result in an upward effect if the federation's level is higher than the service provider requires. Moreover, any new service within the federation with a need for a high or higher assurance level may or will provoke a discussion on the level the federation as a whole needs to authenticate.

3. User-friendliness for the customer. A federation with different assurance levels is relatively less user-friendly. If the user switches over to a service requiring a higher assurance level he will have be authenticated again, comparable to the situation without a federation and without SSO.

**Example**

The service provider determined the desired assurance level for the single service. If only a lower assurance level is available than the service requires, this will automatically lead to denial of access to the service. Service providers may consider adjusting their services so that a lower assurance level may safely be adopted, for example by taking mitigating measures further on in the process.

The Social Insurance Bank [SVB] constitutes a good example of a procedure in which such a solution with a low barrier has been opted for. The services are deliberately designed to require only a Basic DigiD. The consequence, however, is that certain matters cannot be dealt with online or that a letter of confirmation must be sent after completion of the online transaction.

### 8.4.2 User perspective

From the user perspective, whether a citizen or an employee of a business, Single Sign On may lead to confusion. If access is given to different services and a Single Sign Off is not available, sessions may not be terminated immediately. It may not be clear which session is still open at any given moment, which introduces extra security risks.

The service provider using an authentication from a federation may realise the effects of Single Sign On (and Single Sign Off ) on the user and take any necessary actions. This action will take place at the own organisation's level, for example by pointing out the specific effects (and action perspectives) of the use of SSO to the users of their own services. The service provider may also formulate wishes and demands for the federation and thus serve the user better and safer.

This brochure is a publication by:

The Standardisation Forum
November 2013