

Forum Standaardisatie

Exploring Authentication in the Netherlands

Making do with what we have?

KPMG Information Risk Management
Amstelveen, March 2007
This report has 23 pages
R.2007.ISC.18
AvZ/PP/JS/nv

Table of Content

Executive summary	1
1 Introduction	3
1.1 Engagement	3
1.2 Procedure	3
1.3 Assumptions	3
2 Glossary	4
3 Current situation	5
4 The ideal situation	8
5 Opportunities for standardisation and cooperation	9
5.1 Terminology	9
5.2 Quality rating for authenticators	9
5.3 Anchor	10
5.4 Authentication service provider	10
6 Prerequisites	12
7 Conclusion	13
A List of interviewees	14
B Terminology	15
C Authentication service provider	18

Executive summary

Note: This report is a translation in English of the original report, which was drafted in Dutch. In case of inconsistencies, or for interpretation purposes, the original Dutch report prevails.

Looking into the issue of authentication, at the request of the 'Forum Standaardisatie' (standardisation forum, hereinafter: the Forum), it has become clear that people and organisations in the Netherlands have ample means to prove their identity in communications on the internet. ID cards, passwords and biometric information: everyone now has an extensive collection of these so-called authenticators. In other words, no problem, so it appears.

However, a closer look reveals that the current situation with authentication is certainly causing a multitude of problems, such as:

- unnecessary costs for organisations (both government and corporate sector) wishing to perform transactions with their users;
- a growing chance of identity fraud because users have such a multitude of authenticators (a 'digital key ring') that it leads to carelessness;
- a comparatively high threshold for companies that want to conduct reliable business on the internet because they are forced to first set up and then maintain an infrastructure for issuing and managing authenticators.

This situation can be improved by standardising a number of aspects, for example:

- terminology, in order to avoid confusion when communicating about this issue (there are, in fact, numerous definitions for the terms used);
- quality ratings for authenticators, which will make it clear to everyone what degree of security may be derived from the use of a specific authenticator.

In addition, two initiatives have been identified that can also substantially contribute to a healthy practice for authentication in the Netherlands (and abroad):

- using official databases, such as the municipal personal records database (hereinafter: the GBA), the government can issue authenticators to serve as basis for the private sector to issue authenticators;
- setting up a so-called 'authentication service provider' can enable service providers on the internet to use authenticators issued by other organisations. This can reduce users' digital key ring, considerably reduce service providers' costs and it can strengthen the fight against identity fraud. This concept also creates opportunities for the Dutch position in the international field.

It should be added to the above that collaboration between the government and the corporate sector is essential for achieving and making a success of the initiatives. The possibilities available within the responsibilities of the government and corporate sector appear to be good.

‘Making do with what we have?’ No; by sharing what we have, we can develop more power together.

1 Introduction

1.1 Engagement

On behalf of the Forum, ICTU/GBO.overheid has instructed KPMG as follows: explore the opportunities for synergy between and within government authorities and the corporate sector with reference to the identification and authentication of people and organisations in the electronic and internet environment.

1.2 Procedure

This survey was an exploratory one and conducted in the period from February to March 2007. Based on the aim of the survey, an interview questionnaire was prepared and approved by the client. In consultation with KPMG, the client selected eight people who were interviewed by KPMG. A list of the interviewees is attached under Appendix A. In combination with literature, these interviews were used as a source of information for this survey. The overall view created by the information gathered was discussed with the Forum on 7 March 2007, leading to this report.

1.3 Assumptions

The following assumptions were applied to this survey:

- there are numerous definitions for the terminology used in connection with the subject matter of the survey. It is not the intention of the survey to provide definite answers to this;
- the government has the exclusive right and the duty to issue legal means of identification;
- the need for authentication for internet transactions will increase strongly in the coming years;
- this orientation focuses on standardisation that goes beyond that within government authorities alone;
- the technical dimension of authentication is taken as a fact.

2 Glossary

A range of specific concepts are used in this report. The list below provides a simplified definition of these concepts. For those interested, appendix B contains a formal glossary of these definitions.

- Identity fraud: Pretending to be another person (for example, performing unauthorised transactions under someone else's name).
- Identification: Claiming an identity ("I am John").
- Authentication: Proving a claimed identity (for example, using a secret password known exclusively to John and his communication partner).
- Authenticator: The means used for authentication, in other words, something the user knows, owns or is (for example, a password, ID card or a fingerprint).
- Quality level: The degree to which an authenticator provides certainty about a claimed identity.
- Authorisation: Having the authority to perform an action.
- Service provider: A provider of a service that is accessed via the internet (for example, a government website).
- User: A user using or intending to use a service on the internet.
- Issuer: An organisation issuing authenticators.
- Authentication service provider: An organisation, acting as an intermediary for a service provider, dealing with the process of authenticating a user.

3 Current situation

It is up to all service providers to determine whether certainty is required about the identity of the users wishing to use their services and, if so, what degree of certainty they require. Using this as a basis, the service provider then ensures that the user gets an authenticator with which the claimed identity can be confirmed with the desired degree of certainty (Figure 1: The service provider personally issues the authenticators).

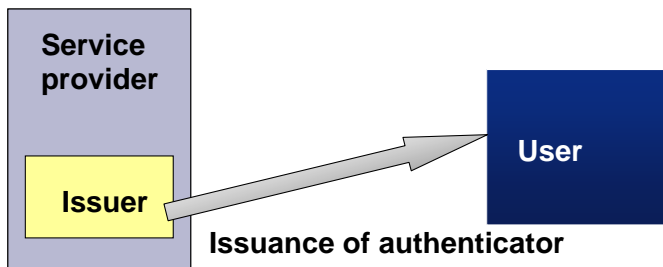


Figure 1: Issuing an authenticator to a user

As the service provider personally issued the authenticator, it can also personally verify the identity of the user before the user performs an action/transaction (Figure 2).

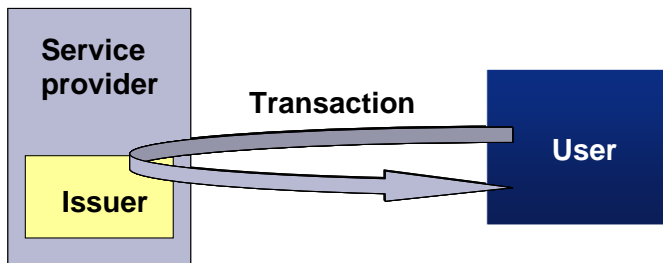


Figure 2: Transaction with authentication

In this way, every organisation in the Netherlands that provides services via the internet takes care of the authentication of its own users; every organisation 'makes do with what it has'.

From the user's perspective, unfortunately, the picture is not quite as rosy (see Figure 3). The current situation means that users are issued with a different authenticator for every service they use. The result is that users now have to remember several passwords and use a series of ID cards. The digital key ring is a fact.

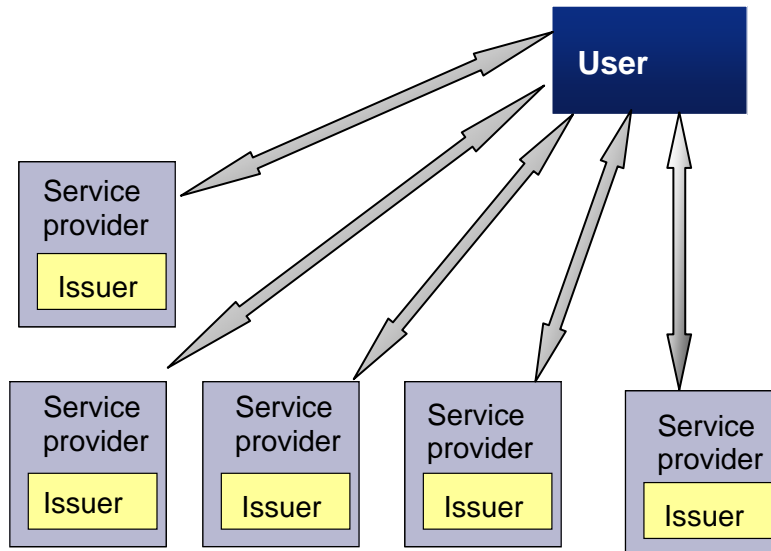


Figure 3: Authenticators of different service providers

Government authorities in the Netherlands have now launched the shared use of the same authenticators (DigiD password, one-time password (OTP) via SMS). Although the government thus contributes towards reducing the size of the digital key ring, one could claim, however, that the government behaves as a large private organisation in which the different divisions, for instance, decide to use the same authenticators. The effect this has on the user's situation for the time being is limited.

The number of communication channels by which users communicate with service providers via the internet continues to increase. For example, using mobile telephones for payments (both transfers and retail), and set-top boxes. This means that the number of authenticators that users need will also continue to increase, also in the form of SMS authentication and smart cards. The introduction of the public transport chip card ("OV-Chipkaart") and the healthcare card also adds to the number of authenticators.

A large digital key ring is not ideal for various reasons:

- users have so many authenticators that they becomes difficult to manage properly and form obstacles to easy use. This could also hamper the use of the available services;
- the multitude of authenticators (mostly passwords) means that it will become inevitable for most users to write these down to remember them. The quality level of each authenticator is also not clear to the user. Moreover, the abundance also means that the average user will not be interested in finding out more. All of this means lesser quality of the authentication and also an increasing chance of identity fraud.

At the moment, there appears to be no issue from the individual service provider's perspective; after all, it is possible for the required authentication to take place. However, closer inspection reveals that:

- various service providers claim that the costs associated with issuing and managing authenticators are higher than they consider acceptable because every service provider has to design, maintain and manage its own infrastructure;
- various service providers see the cost as an obstacle to introducing authentication or to upgrading to stronger authenticators. This can be concluded from recent requests to existing issuers (such as government authorities and banks) for permission to use their authenticators.

From the government's perspective, too, the current situation leads to unwanted effects. The rise in identity fraud is a cause for concern that deserves appropriate action from the government, among others.

These issues are widely acknowledged. There have been numerous reviews and meetings, and all sorts of initiatives have been launched, such as the introduction of the DigiD password and DigiD as the authentication service provider for government organisations. We also notice a trend within large organisations to reduce the number of authenticators used internally and issued to clients.

However, these remain isolated solutions: each service provider tries to improve its own situation and that of its users. This does not resolve the issues outlined in this section. Users are left with expanding digital key rings and services providers continue to face unnecessarily high costs.

In the end, the users (people and organisations) pay the bill, because the costs of all the infrastructures are ultimately passed on to the users. The result is an increase in the burden of costs, whereas a reduction is called for.

The next section sketches the characteristics of an 'ideal' situation in which the outlined issues have been resolved.

4 The ideal situation

Not only in the Netherlands, but also abroad, it has been acknowledged that the situation with authentication can be tackled more effectively than having each service provider issuing its own authenticator. Examples inside Europe include Austria, Denmark, Sweden, Finland, Estonia, Italy and Malta, with a solution to the issue being sought in cooperation between the government and the corporate sector.

Partly by virtue of insight gained from abroad and from the survey, a number of characteristics of the 'ideal' situation have been identified.

- It is up to individual users to decide the size of their digital key ring because service providers reuse existing authenticators and registration and issuing processes as widely as possible. This means that new service providers are not required to issue their own authenticators and, therefore, are not 'punished' by the need for considerable investments in the design, maintenance and management of their own infrastructures if they wish to combat identity fraud. Moreover, by using technological developments, it is possible to rapidly create critical user mass.
- The quality of the authenticators is clear, both to service providers and to users.
- The government is responsible for authenticators in the electronic environment that were issued on the basis of official databases. The government can thus lay the foundation for strong private authenticators, among other things, for combating identity fraud. This creates a parallel with the use of passports in the physical world with its roots in the official databases (such as the GBA) in the Netherlands.
- The process and the means applied in the Netherlands for authentication are in line with international developments in this field. Service providers, users and issuers all increasingly work on an international scale, as the internet is not bound by national borders.

The following section looks at areas where government and corporate sector can join forces in standardisation and cooperation to change the current situation to one that meets the characteristics specified above.

5 Opportunities for standardisation and cooperation

Various forms of standardisation can make a significant contribution to solving the issues outlined in section 3 and to taking steps in the direction of the 'ideal' situation as far as authentication is concerned. To succeed in achieving this standardisation, the government and the corporate sector will need to work together closely in order to set users (people and organisations) free from the growing digital key ring. Sections 5.1, 5.2 and 5.3 describe the proposed initiatives. All these initiatives should take into account that the situation achieved should be a close match to the international one. This will avoid the results of initiatives only being applicable to the Dutch situation.

It should additionally be the aim to achieve a joint initiative between government and the corporate sector in this context that would present a significant step forward. A proposal for this is included under 5.4.

5.1 Terminology

The success of the debate about agreeing an authentication policy depends on the clarity of the communication about this issue. All the parties involved should therefore use the same terminological framework. We recommend agreeing this framework in consultation between the government and corporate sector.

The term 'DigiD' deserves a special mention and also requires some explanation. At the moment, the same term is used for:

- the authenticator issued by the government (the DigiD password);
- the technical platform facilitating the authentication process for service providers in government authorities (DigiD as authentication service provider);
- the organisation responsible for the two aforementioned facilities.

This causes unnecessary confusion and we therefore recommend making a distinction between the three aspects listed above.

5.2 Quality rating for authenticators

To clarify the differences in quality of authenticators, it is worthwhile creating quality ratings as a clear indication of the strength of the authenticators. It should also be determined which criteria authenticators need to satisfy in order to be 'approved' for a specific rating, and which organisations are qualified to perform these assessments.

In addition to the initial steps, authenticators should then be 'rated' using a uniform process.

To ensure proper understanding, communication concerning quality aspects and criteria to service providers, users and issuers should also be clear and unambiguous.

5.3 Anchor

An important aspect in issuing authenticators is the registration of the user, with the connection being made between the authenticators and the identity. The government can fulfil a major task in this. Issuing authenticators based on the official databases creates a good, uniform basis for private parties to issue their own authenticators. Private parties can thus use this 'standard' to standardise their own registration and issuing processes. This means reducing costs and increasing the ease for users because of greater uniformity.

To the extent not yet provided for above, the government could further consider taking the responsibility for issuing at least one authenticator in each rating category (see 5.2., as well as 5.4.).

5.4 Authentication service provider

A significant step forward can be taken if a service provider is no longer required to issue an authenticator by itself but instead use an authenticator already issued by another organisation. In this case, all a service provider still needs to do is to specify the desired quality level of the authenticator, which is possible by creating a so-called 'authentication service provider'. For a more detailed explanation of this concept, please refer to Appendix C.

Technically, such an organisation is comparable with the current DigiD platform, but with the following differences:

- it provides authentication services for all market parties and the government;
- it basically offers the option to use all the authenticators available in the market provided they satisfy a specific quality rating on the basis of approved criteria.

This includes the following.

- service providers can use the authentication service provider to deal with the authentication of 'their' users and no longer need to incur the cost of issuing and managing their own authenticators. Service providers can thus 'tap into the resources' of other providers rather than having to make do with what they have;
- it becomes possible to reuse authenticators, with issuers of such tools being able to break even through other organisations using the tools;

- it is up to users personally to decide which authenticator they wish to use for verifying their identity, thus needing only a small digital key ring;¹
- through a strict segregation between the service provider, the issuer and the authentication service provider, users retain personal control over access to their personal data by third parties;
- this will enable a more effective regulatory role for the government than currently is the case, for example, with respect to privacy. In the end, the number of authenticators and parties involved will be considerably smaller than at the moment;
- the financial burden can be reduced.

To ensure a workable situation, the creation of one or more authentication service providers means that it must be possible for both service providers and issuers to communicate with the authentication service provider via standardised interfaces. This will increase competitiveness and transparency.

Moreover, users and service providers will need to have sufficient confidence in the authentication service provider (including from a privacy perspective) which, in turn, requires proper regulation of the authentication service provider(s). It would therefore be sensible to set up a regulatory entity for this.

The elaboration and realisation of this concept can be launched with a small group of service providers and issuers. In this context, it must be ensured that the practical implementation does not stand in the way of full development to integral use. If the concept of the authentication service provider proves to be successful, more and more service providers will start using it (and withdrawing authenticators issued in the past), and issuers of authenticators will want their authenticators approved.

Besides the initiative outlined above, the government can also make a significant contribution to this development by:

- having the DigiD technical platform also accept authenticators not issued by the government. This will enable users to communicate with government authorities using authenticators already in their possession;
- offering the DigiD technical platform also to service providers that are not government organisations.

This initiative can be a significant boost internationally to the Dutch position on authentication. There is considerable interest abroad in a concept as outlined above.

¹ It is not realistic to expect that the number of authenticators can be restricted to one. After all, some organisations will want to use their authenticator to increase their brand familiarity. However, the existence of an authentication service provider will force organisations to reconsider the issuing of their own authenticators and the benefits it offers, like brand proliferation.

6 Prerequisites

There have been many attempts in recent years to resolve the problems surrounding authentication in the Netherlands. Time and again, these efforts have run aground on the lack of resolve or trust. The present orientation is the impetus to a new initiative. The lessons from the past teach us that it is only worth an attempt if the preconditions below are satisfied:

- a clearly identifiable coordinator should be assigned who is responsible for resolving the fundamental issue;
- it must be clear who is responsible for the realisation of the agreed objectives;
- the government and the corporate sector will have to jointly agree the standards referred to under 5.1 and 5.2 in order to create sufficient support;
- sufficient parties have to be willing to join right from the start to make a success of the concept of an authentication service provider;
- parties involved in the partnership must have sufficient confidence in one another;
- there should be proper harmonisation with international developments.

If these preconditions are not satisfied, it does not seem wise to continue to pursue crucial collaboration between the government and the corporate sector in the field of authentication. Other countries in Europe will then eventually come up with initiatives which the Netherlands can or must join.

7 Conclusion

Given its exploratory nature, this report only offers outlines. It does not aim to offer a fully detailed project for resolving the identified issues.

During our work, it became clear that all those involved recognised and acknowledged the problems. Despite numerous attempts, no structural solution has yet been found.

The direction proposed in this report could offer such a solution. If the government and the corporate sector joined hands with vigour and in unison, the Netherlands can make significant achievements in the field of authentication. Users (both people and organisations) and service providers can then reap the benefits offered by electronic communication with more ease.

By joining forces, we can achieve more.

If you have any further questions, please do not hesitate to contact us.

A. van Zanten CISA
Partner, KPMG Information Risk Management
KPMG EDP Auditors N.V, Amstelveen, The Netherlands

A List of interviewees

Name	Organisation
G.B.J. Hartsink	ABN AMRO
S. Luitjens and E. Hardam	GBO.Overheid
C. Franke	Centre for Work and Income
T. Masseur	Thuiswinkel.org
Dr. P.W.J. de Graaf	VNO NCW
W.C. Westerhof and F.J.H. Visser	Rabobank
Dr. H.J.M. van Zon and T. Meesters	Ministry of Home Affairs
M.J.P. Stoelinga	Association of Chambers of Commerce

B Terminology

Various concepts are used in this report, the most important of which the definitions are listed in this appendix. In almost all instances, several acceptable definitions are in use for the terms. The definitions for this report were selected where possible on the basis of sources used by the European and other authorities.

B.1 Context of the use: Objects

Entity – “An entity is anyone, natural or legal person, or anything [*e.g. a computer*] that shall be characterised through the measurement of its *attributes*.²”

Identity – “The identity of an entity is the dynamic collection of all the entity’s *attributes*. An entity has only one identity.³”

The identity consists of a number of attributes that need not necessarily be unique for that entity. Despite possible ambiguity, a combination of attributes is nonetheless useful when attempting to distinguish several entities. The more certainty required, the more and stronger distinguishing attributes have to be evaluated.

Attribute – “An attribute is a distinct, measurable, physical or abstract named property belonging to an entity.⁴”

An attribute has a type and a value, it is any piece of information about an entity. A set of attributes does not necessarily uniquely distinguish the entity from any other entity; however, the number of attributes and the distinguishable property do contribute to it.

Authority – “The permission of an authenticated entity to perform a defined action or to use a defined service/resource.⁵”

Identifier – “An identifier is an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context.”

Authenticator – “An authenticator is a set of attributes delivered by an entity, the authenticity of which is assessed through a specific process.”

In the context of identification and authentication, the terms ‘identifier’ and ‘authenticator’ are used synonymously by many people. Although, technically speaking, both terms describe the same attributes, there is a difference in the application of the tool. An identifier is used to *claim* an identity; an authenticator is used to *corroborate* a claimed identity.

² Modinis, Study on Identity Management in eGovernment (2005)

³ Modinis, Study on Identity Management in eGovernment (2005)

⁴ Modinis, Study on Identity Management in eGovernment (2005)

⁵ Modinis, Study on Identity Management in eGovernment (2005)

B.2 Context of the use: processes

Creating an identity – “An identity is created by recording a set of attributes of an entity and linking these to this identity. The full set of attributes forms the identity.”

Identification – “Identification is the process of using claimed or observed attributes of an entity to deduce who the entity is.⁶”

Authentication – “Authentication is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence.⁷”

The authentication process involves the corroboration of a set of attributes to confirm, with a specified level of confidence, whether a claimed identity corresponds with the actual identity of an entity. This can involve the corroboration of a set of observed or claimed attributes (such as a password, token, biometrics, telephone number, etc.).

Authorisation – The permission of an authenticated entity to perform actions (such as reading, adjusting or editing) on information or resources.⁸

This process involves defining the authorities of an entity whereby an entity is granted permission to perform a specified action or to use a specified service or resource.

Interoperability – The possibility for different electronic systems to work together with one another.⁹

In the context of identification and authentication: Interoperability is defined as when a service provider is not part of the technical and legal ‘sphere’ of the party that has recorded the identity of an entity, and when the claimed identity can be verified with this party by a trusted third party.

The following conditions apply:

- 1 the identity can be read and interpreted by the service provider (technical condition);
- 2 the service provider gives permission for the entity to perform the required action or to use the required services or resources.

B.3 References

For this project, we looked for generally accepted definitions. Reference was made in particular to the terminology used in PKIoverheid in the Netherlands and the interim result of a study conducted on behalf of the European Commission into ‘Identity Management’:

⁶ Modinis, Study on Identity Management in eGovernment (2005)

⁷ Modinis, Study on Identity Management in eGovernment (2005)

⁸ PKIoverheid (2005)

⁹ PKIoverheid (2005)

- 1 Modinis, “Study on Identity Management in eGovernment” for the European Commission, November 2005;
- 2 PKIoverheid, Programma van Eisen, deel 4.
http://www.pkioverheid.nl/uploads/media/PvE_deel4_v1_0.pdf, 2005.

C Authentication service provider

If we removed the need for service providers to personally issue an authenticator and instead use an authenticator already issued by another organisation, it could be an important step towards resolving the problems around authentication, which is possible by creating a so-called 'authentication service provider'.

The authentication service provider offers an infrastructure for validating the identity of users with the aid of different authenticators, possibly issued by third parties. In this sense, the authentication service provider is technically comparable with the DigiD platform, but also available to private parties.

C.1 Processes

The authentication service provider model is illustrated in Figure C1.

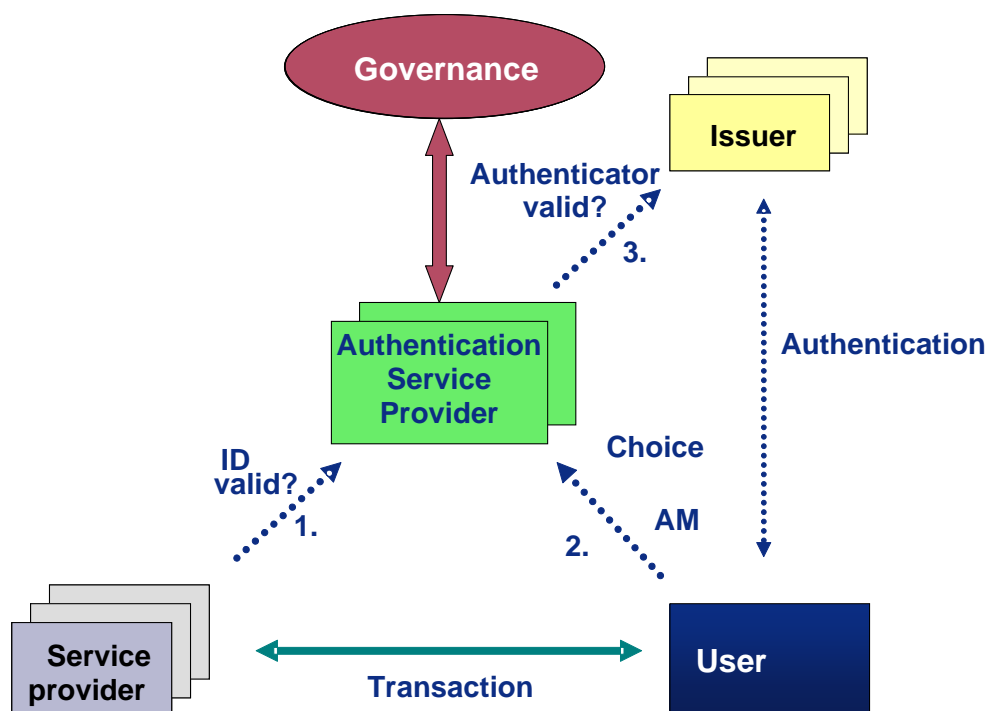


Figure C1: Authentication service provider model

Besides the authentication service provider itself, another 'new' party is also introduced in this model: the issuer of authenticators. This role was previously performed by the service provider itself, but in the new model, the issuer can be both a third party and the service provider itself.

The model roughly works as follows: If a user and a service provider wish to conclude a transaction, the service provider determines whether authentication is required and, if so, the level of certainty to be provided by the authentication. The model then goes into operation.

Step 1 – The service provider submits a request to validate an identity against a specified quality level.

The service provider contacts the authentication service provider and submits the request. The service provider names the user and specifies the quality level required for the authentication. Please note: the service provider is not concerned with the authenticator to be used in the process. The service provider only specifies the quality level required.

Step 2 – The user selects an authenticator to prove the identity.

The authentication service provider then contacts the user to enquire about the authenticator to be used. The authentication service provider also indicates the quality level. The user then selects one of the available authenticators of that quality level to be used in this transaction.

In practice, users will have informed the authentication service provider in advance of the authenticators at their disposal.

Step 3 – Issuer validates the identity on the basis of the chosen authenticator.

This step involves the actual process of authenticating the user. Based on the user's choice, the authentication service provider establishes who has issued the authenticator. The authentication service provider asks the issuer to verify the identity of the user in question.

To this end, the issuer contacts the user and performs the validation, for example, by asking for the user's password or by checking whether the user is in possession of a valid card.

The issuer reports the result to the authentication service provider which, in turn, reports to the service provider. If the result is positive, the service provider and the user will conclude their transaction.

C.2 Standardisation

To guarantee the success of the outlined model, the following standardisations are required:

- the different quality levels (levels of trust) of the authenticators will have to be specified;
- clear criteria will have to be defined for each quality level for accepting authenticators in that quality level;
- guidelines should be agreed on how service providers, authentication service providers and issuers will know which user's identity to validate;

- to enable interoperability and competition, standardised messages must be set up between the service providers, authentication service providers, issuers and users.

C.3 Advantages

This model offers the following advantages:

- For the service provider:
 - When performing a risk assessment to determine the desired quality level to be offered by the authentication process, service providers can use the classification of the authenticators.
 - Service providers can use all the authenticators on the market. Service providers therefore need not issue their own authenticators and can provide their services without first having to set up an infrastructure for authentication.
 - Service providers can avoid large investments in this way and, for instance, only need to pay a sum per authentication to the authentication service provider.¹⁰
- For the user:
 - Users can use authenticators that have been approved for a specified quality level at different service providers, thus limiting the size of their digital key ring.
 - Users personally select the authenticator they wish to use to verify their identity with every transaction they perform with a service provider.
 - By using the quality rating for authenticators, it becomes clear to the users what level of trust the authenticator offers.
- For the government:
 - The number of authenticators will probably decrease in the long term because the need for service providers to have their 'own' authenticators will disappear. Moreover, the quality of authenticators is rated and the quality level of these tools is also clear to the user. This makes an important contribution to combating identity fraud.
 - The reuse of authenticators means that government authorities will also face lower costs for issuing authenticators. Some of the people and companies will, after all, use authenticators issued by private parties in their communication with the government. This means cost savings for government authorities.

¹⁰ This obviously depends on the commercial payments system set up by such an authentication service provider.

- Furthermore, the Dutch public as a whole will face lower costs for setting up, maintaining, managing and using authenticators, which means a lighter financial burden.
- For issuers:
 - It becomes possible to reuse authentication tools, with issuers of such tools being able to break even through other organisations using the tools;

C.4 Observations

The model for the authentication service provider does, however, call for some annotations.

- It is not feasible to present this model in detail in the context of this exploration of ideas, and the above should also be seen as an outline.
- The parties in the model must be able to ascertain which user's identity has to be validated. It is vital to select a solution that will not infringe on the privacy of the user. Although it is possible for the authentication service provider to identify the service provider with whom the user communicates and the authenticator the user utilises in the process, the authentication service provider does not receive any information about the content of the communication between the user and the service provider (the 'transaction').
- The last point does, however, require that the authentication service provider be subject to regulation, because even knowing with which service providers a user communicates is sensitive information. Independent regulation must ensure that the service providers and the users have and maintain the necessary confidence in the model.
- The standards required for the model's operation should be produced and maintained by an entity that is not an authentication service provider itself in order to avoid a dominant position being created. The regulatory body referred to above could play an important part in this (and in monitoring compliance with the standards).
- There is no principle objection to several authentication service providers operating alongside each other. Whether this will indeed be the case will probably depend to a large extent on commercial factors. The model is however ideally suited for use in other countries. In that case, a network of authentication service providers could lead to international competition and standardisation. The Netherlands can take the lead in this.