Colophon

Project Name **Expert Advice public interface eRecognition v1.4**

Version Number 1.0

Location

Organization Standardization Forum

PO Box 96810

2509 JE Hague

forumstandaardisatie@logius.nl

Authors

Jaap Kuipers

Michael van Bekkum

This document was translated using Google's translation service for Kantara Initiative eGov WG by Rainer Hörbe. This original document was retrieved at:

https://www.forumstandaardisatie.nl/fileadmin/os/Consultatiedocumenten/120806_Expertadvies_eHerkenning_overheidskoppelvlak.pdf

Content

Executive Summary

What is the conclusion of the expert?

The expert advises majority government standard interface eRecognition, version 1.4, to include on the list of 'comply or explain' if the following condition is satisfied:

• Mention and publish the provisions regarding intellectual property and trademark rights in addition to the documentation of the standard.

With the scope:

"Authentication for Web services of public services to businesses and organizations and to establish the authority of the requested service."

And if scope:

"Governments (central government, provinces, municipalities and water boards) and institutions in the (semi-) public sector."

At the time of writing, speaking three parties, namely the Tax Logius and the Ministry of the Interior is not yet on inclusion in the list.

Supplementary advises the expert management organization eRecognition to ensure:

- Publication of the version adopted policies in addition to the documentation of the standard.
- Provide insight into the changes to the standard in the different versions of documentation.
- Public availability of the documentation of the standard without notification process.

The expert group has no further risks identified.

What is the substance?

The default public interface eRecognition describes the interface between the (government) service and the eRecognition Broker Via the interface receiving government organizations identification and authorization information about representatives of companies / organizations for access to web services by the same government organizations are provided.

The government eRecognition interface is thereby part of the appointments system eRecognition. The appointments system is a set of rules by which parties in a network to deliver eRecognition Services. In this network, the parties share authentication means that publishing, authentication services, and act as a registry for powers brokerage grant eRecognition.

The government eRecognition interface approach the problem of the diversity of authentication facilities for separate administrations to solve ("keys"), allowing companies as users are faced with many choices and non-standardized consistency between the technical interfaces. In the past, while the Standardisation Forum expressed the desire to achieve better frames around identification, authentication and authorization. eRecognition such a framework, in accordance with the advice of the Advisory A3 Authentication and Authorization Companies.

How did the process go?

On 2 July 2012, an expert group with representatives from industry and government met. Pre-existing experts and others who could not attend, the

opportunity to provide input. Based on this input and the discussion during the meeting prepared this advisory.

How successful is the standard on the evaluation criteria?

Open standardization process

The documentation is available after registration, the decision procedure is sufficiently accessible, there is an appeals procedure and the standardization organization is independent and sustainable. The standard conforms to the opinion of the expert, however, only to the openness criteria as well as the following condition is met:

• The rules applicable in respect of intellectual property (trademark and) should be raised and should supplement the current documentation of the standard are published.

Added value

The expert believes that the benefits of government eRecognition interface outweigh the risks and disadvantages: the government-wide and societal benefits outweigh the costs, and privacy and security risks in the standard is sufficiently covered. The standard also provides added value compared to the standard SAML v2.0. The advantages of the standard public interface eRecognition are particularly reflected in the reduction of the diversity of authentication features and the contribution it makes to reducing interoperability problems in this area. The interface is also an independent top SAML profile also turn off the system to eRecognition.

There are alternatives to the standard, but these are less easy to use, be phased out or know much lesser extent, embedding into an elaboration of rules and agreements (such as the appointments system eRecognition) to correct and interoperable use of the standard guarantee.

Support

The expert believes that there is sufficient support for the standard, there is support for the market standard by multiple vendors, and there is policy support for eRecognition in iNUP and Digital Agenda.nl. The number of affiliated providers of public services at the time of writing about 40 (44 administrations) and increases in number.

Inclusion promotes the adoption

Placement on the 'comply or explain' list confirms the government developed and implemented policies to achieve a rural herkennings-/authenticatiedienst. An obligation through 'comply or explain' sees the expert also as a means of iNUP and Digital Agenda made policy goals and administrative arrangements actually achieve and the use of the eRecognition standard practice to promote.

What additional advice there regarding the adoption of the standard?

For inclusion in the list there is some overlap with the standard SAML already on the 'comply or explain' list. Recommendation of the expert to the Forum:

• To pay attention to the relationship between standards in the field of identification, authentication and authorization and to examine how these two standards relate to each other in a framework for this domain.

A recommendation that the expert does the management organization for eRecognition is:

• examine how the application of SAML and public interface eRecognition can be better coordinated and, where necessary, a proposal for an alternative definition.

A recommendation that the expert does Logius and eRecognition jointly:

• to ensure consistency (and in particular the consistency in a number of technical choices) between DigiD and eRecognition mapping and where possible improve.

1 Objective expert advice

1.1 Background

In 2007, the Cabinet approved a plan Netherlands in Open Connection [1]. The purpose of this Action Plan is to facilitate access to information, independence from IT vendors to create and pave the way for innovation.

One of the measures of the Action Plan is to use a list of standards which fall under the principle "comply or explain" (comply or explain) [2]. The Standardisation Board, in 2006 the government set up, speaks out about the standards that will be included on the list, including on the basis of an expert assessment of the standard [3]. The Standardisation Board is advised by the Standardisation Forum. Office Standardization Forum supports both institutions.

Fourteen experts gathered in an expert group that the standard has assessed a number of criteria. These criteria - pre-determined by the Standardisation [4] and elaborated in the form of specific questions - in the here present expert advice mentioned and discussed.

Subject of this expert opinion is the default state interface eRecognition v1.4. This standard has been notified by mrs. Paula Winter behalf of Ministry EL & I for inclusion in the list of open standards 'comply or explain'. The assignment of the expert group was to draw up an opinion on whether or not to include this standard in the list, whether or not under certain conditions.

1.2 Process

For the preparation of this opinion is the following procedure:

- Through the Office Standardisation Forum on March 5, 2012 an intake interview with the applicant. This is the standard tested on exclusion criteria (criteria for treatment in particular ') and a first estimate of the chances of success for recording.

- Based on the intake has decided to set up an expert group. On the basis of this decision by the Bureau Standardization Forum assembled a group and president sought. On the basis of the notification and the intake is a preparation dossier prepared for members of the expert.

- The expert started individually scoring the default public interface eRecognition v1.4 using a spreadsheet with questions in preparation file. Based on the obtained answers president and supervisor of the expert group identified various bottlenecks.

- Next, the expert on 2 July 2012 and discussed the findings in general and the identified bottlenecks in particular to discuss. During this meeting, also the application and scope determined.

The results of the expert by the president and counselor included in this advisory report. A first draft to the members of the expert sent with a request for comment. After processing the responses, the report is completed, again sent to the experts and submitted for public consultation.

1.3 Continued

This expert opinion is in favor of a public consultation be made public by the Office Standardization Forum. Any person may, during the consultation period

on this expert advise his / her comment. The Office Standardisation Forum then explains the reactions to the Chairperson and, if necessary, to the expert.

The Standardisation Forum will be based on expert advice and relevant insights from the public consultation an opinion on the Standardisation drawing. The Standardisation Board ultimately decides on the basis of the opinion of the Board or the standard the 'comply or explain' list is.

1.4 Composition expert

For the expert group were invited persons who through their personal expertise or work in a particular organization directly or indirectly involved in the standard. In addition, an independent chairman appointed to the expert to lead and to act as responsible for the final expert advice.

As president has occurred mr. Jaap Kuipers. He has 10 years experience in the field of authentication services, including in relation to eRecognition, DigiD and other large facilities. He is the initiator of the Platform Identity Management Netherlands and independent identity management consultant for, among other ECP.nl and international projects.

The expert group commissioned by the Standardisation Forum accompanied by mr. Michael van Bekkum, standards and interoperability consultant at TNO.

At the expert participated:

- Mr. Jeroen de Beer (Anoigo)
- Mr. Siem de Bruijn (Digidentity)
- Ms. Nicole Damen (Management Organisation eRecognition)
- Mrs. Welmoed Fokkema (Logius)
- Mr. Peter Johan Groeneveld (CapGemini)
- Mr. Indra Henneman (Management Organisation eRecognition)
- Mr. Gershon Janssen (Aviation Industry)
- Mr. Martijn Kaag (Connectis)
- Mr. Wim Kegel (Logius)
- Mr. Saam de Mooij (Min. BZK)
- Mr. Rob Hans de Reus (Tax)
- Mr. Ronald Siemonsma (CJIB)
- Mr. Michael Stoelinga (Management Organisation eRecognition)
- Mr. Kick Willemse (Evidos)

If listeners were present:

- Mr. Nico Baarsen (HEC)
- Mrs. Marjolein Minderhoud (HEC)
- Mr. Mano Radema (HEC)
- Maarten van der Veen (Logius, Office Standardization Forum)

In addition, a number of people a substantive contribution by the individual scoring of the standard or by giving a written reply in general terms:

- Mr. Maurice van Erven (KING)

- Mr. Bob Hulsebosch (Novay)

- Mr. Hans Zandbelt (Ping Identity)

Their contribution is included in the discussion in the expert group.

1.5 Explanation interface eRecognition

The default public interface eRecognition v1.4 describes the interface between a (government) service and the eRecognition Broker. Through the interface receiving government organizations identification, authentication and authorization over companies and organizations and their representatives, for the purpose of access to web services that are delivered by the same government organizations.

The government eRecognition coupling surface v1.4 is a part of the system arrangements eRecognition. The appointments system eRecognition is the set of agreements in the field of organization, control, monitoring, management, architecture, applications, technology. procedures and rules for a network of cooperating parties. In this network, the parties share authentication means that publishing, authentication services, and act as a registry for powers brokerage grant eRecognition.

eRecognition is a standardized, electronic means of authentication of companies and organizations, when digital services from (government) service providers (such as DigiD authentication means that now is for citizens). eRecognition allows the exchange of those data to the relevant parties to authenticate, identify and authorize.

Any provider who meets the requirements, can eRecognition connect. Because the current (first) public service providers are defined as within the scope of this report, the term also public service provider.

The eRecognition system approach the problem of the diversity of authentication facilities for separate administrations to solve ("keys"). These are companies like user faced with many choices and non-standardized consistency between the technical interfaces. Companies and other organizations can eRecognition with multiple service visit and have thereby no longer any task other means of authentication required. The service provider in turn knows by eRecognition with which the service consumer (business) it does business and whether the person is authorized to act on behalf service consumer to do business with the provider. The service provider itself does not have its own authentication tool to view and manage.

The appointments system eRecognition contains provisions on the to provide services, the types of roles in the network and the relationships between those roles. Furthermore, the agreements on the precise functioning of the network: technical relationships, supported functionality, quality of data and services. There are agreements on the underlying infrastructure: what standards are applied, and what messages and interfaces are supported.

The default public interface eRecognition v1.4 describes the interface between the (government) service and the eRecognition Broker within the system. The eRecognition Broker delivers eRecognition Services based on the network eRecognition to government service. The coupling plane, is fed by any

eRecognition Broker implemented and offered to its users, the service providers. The interface implements the use case "Authentication acting customer service".

In this use case, the identity of the agent service consumer, the (pseudo-) identity of the acting individual and the authority of the acting natural person acting on behalf of the service recipient adopted. The eRecognition Broker will make a statement on the service. The location of the interface in the system eRecognition is shown in the figure below.

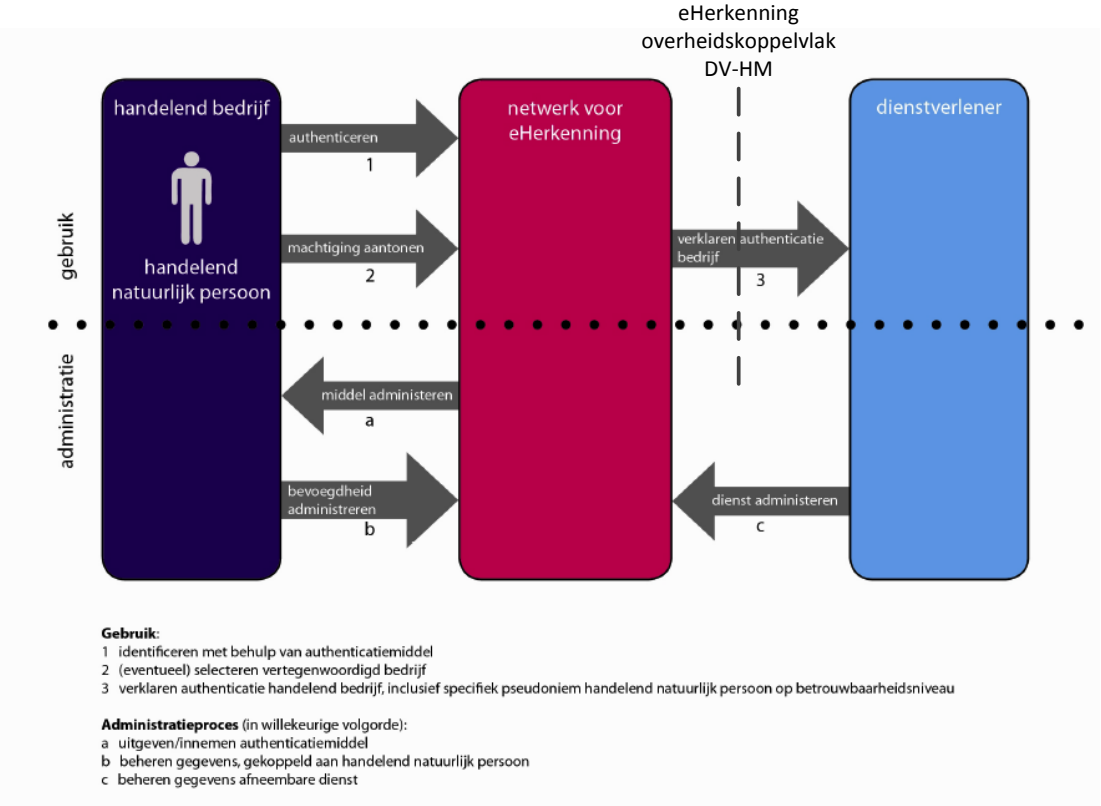

Figure 1 Location of eRecognition public interface in system eRecognition

1.6 Relationship with other standards

There is a relationship with a number of other standards:

appearing on the list of open standards 'comply or explain':

- SAML

The eRecognition interface is a specific profile SAML v2.0, an XML-based standard for the exchange of identity information such as authentication, powers and attributes between different domains.

- ISO27001 / 27002

The eRecognition interface has no direct relationship with ISO27001/27002 that requirements specify for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the overall business risks to the organization . In the design of the system is taken into account the objective of certification achievable in systems that make the appointments system implementation.

appearing on the list of common open standards:

- HTTP

in eRecognition specifies the bindings of SAML 2.0 are required (HTTP POST mandatory, others optional).

- SHA-2

In eRecognition is (at least) using the SHA-256 hashing algorithm (part of the SHA-2 family).

- TLS

All connections for eRecognition interface must use SSL 3.0 or TLS.

- XML

eRecognition uses XML for the specification of the messages that are exchanged via the interfaces.

- UTF-8

For all messages sent through the interface eRecognition be exchanged, should be used with the Unicode character set UTF-8 encoding.

1.7 Structure

Chapter 2 describes the cases in which the standard would be used functionally (functional scope) and by which these organizations should be used (organizational scope).

To determine whether the standard should be included on the list of standards for 'comply or explain', it is assessed against four criteria defined by the Standardisation. Chapter 3 contains the results of this review. Chapter 4 contains a summary of the test results and the opinion of the expert to the Standardisation Forum.

2 Application and scope

Government organizations are expected to adopt the list of open standards in tendering procedures under the "comply or explain" regime. Depending on the purchasing function will have to be determined which interfaces must be implemented, and what standards from the list above should be used. In order to do this, the expert examined the cases in which standard should be used functionally (functional scope), and by which these organizations should be used (organizational scope).

2.1 Functional scope

The expert for the scope of the public interface eRecognition some characteristics and principles established:

- The standard focuses on the state of the authentication for electronic services.
- The standard is applicable to access to electronic services through web technology.
- Services includes both information services, interaction services and transaction services where authentication is required.
- The eRecognition public interface should be applied at the interface between the (government) service and recognition broker.
- For exchange of authentication information on behalf of companies, with a corresponding authorization statement.

If functional scope is therefore proposed:

"Authentication for Web services from government agencies and service providers to establish the jurisdiction of the requested service."

Notes to the definition:

- Among organizations understood here means natural and non-natural persons who are registered in a commercial register. This means that besides the companies also associations, foundations and (parts of) government organizations can relate. The application is limited to the interface between the providers of identification services and the aforementioned public service.
- The power is determined by reference to the interface via the authorization data exchanged, including a statement about the power of acting, natural person.

2.2 Organizational scope

The expert group recommends the organizational scope to match the scope in which the 'comply or explain' principle applies, namely:

"Governments (central government, provinces, municipalities and water boards) and institutions in the (semi-) public sector."

The above description of the operation field contains the opinion of the expert, directly or indirectly, all relevant parties to whom the standard applies. The expert saw no reason for the above scope further restrict.

3 Assessment of standard criteria

To determine whether the standard should be included on the list of open standards that are tested against a number of criteria. There are four main criteria:

1. Open standardization process
2. Added value
3. Support
4. Recording promotes adoption

These criteria are described in the report, "Assessment Procedures and Criteria for lists of open standards" [2] and on the website www.open-standaarden.nl. The outcome of the review in this chapter will be described for each criterion. For completeness, also the definition of each criterion.

3.1 Open standardization process

The development and management of the standard in an open, independent, accessible, insightful, careful and sustainable design.

3.1.1 Is the documentation for each threshold freely available?

3.1.1.1 Does the specification document available without the existence of unacceptable barriers (like excessively high costs and high membership requirements)?

3.1.1.2 Is the documentation of the development and management process (eg provisional specification document, records and description decision procedure) available without the existence of unacceptable barriers (like excessively high costs and high membership requirements)?

Both specified ocument as other documentation after registration at no cost to download from the website www.eherkenning.nl. For obtaining the documentation is no membership required.

The expert notes that it is desirable that the documentation is made available publicly without signup process, because the registration procedure and the data are collected at registration no obvious contribution to adoption of the standard.

3.1.2 Is the intellectual property available to individual citizens, so that the standard freely implementable and use

3.1.2.1 Sets the standardization organization the intellectual property rights in the standard for any such patents, irrevocable royalty-free for everyone available?

Part of the private law provisions in the legal framework of the agreements eRecognition system is that all intellectual property matters by the managing organization are developed to the managing organization or its licensors. As a non-profit organization that publishes full appointments system is the management organization for availability.

There are no restrictions on the use of the standard in other domains. The use of the brand name eRecognition are restrictions imposed. The right to use the mark eRecognition is subject to the conditions that a Participant to all liabilities, including those of the interface, the appointments system and meets the Participants Agreement has been signed. Now if only the interface DV HM is

used outside the appointments system and adjustments are made in this is no problem, but if this is not under the umbrella of eRecognition used.

Regarding the use of SAML within the standard public interface eRecognition, further apply the provisions set out in the Intellectual Property Rights (IPR) policy of OASIS are listed. Furthermore, the former expert in the expert advice for SAML 2.0, in respect of intellectual property already noted that "sufficiently fulfilled this criterion, although strictly speaking, patents are not irrevocably made available. "

Prior to the opinion of the expert on this criterion, a point with respect to management to be solved:

• The rules applicable in respect of intellectual property (trademark and) should be raised and should supplement the current documentation of the standard are published.

3.1.2.2 Ensures the standardization organization that parties that contribute to the development of their standard intellectual property irrevocable royalty-free for everyone available?

There will apply to contributions by the parties involved in the development of the standard, no other rules than mentioned above. That is, that these contributions be made available to the abovementioned reservations concerning the brand eRecognition.

3.1.3 Is the participation of everyone adequately secured?

3.1.3.1 Is the decision-making accessible to all stakeholders (eg users, suppliers, consultants, academics)?

The participating parties eRecognition have control over the content and development of all parts of the system eRecognition agreements, including the public interface. This control by parties within the Appointments System eRecognition takes place at the strategic, tactical and operational levels, as defined in the "Decree establishing control eRecognition" These three levels are three consultative bodies set: the System Council, the Tactical and Operational Consultation Consultation. These forums are the parties involved eRecognition at the table, through a delegation of participants (Party producing one or more roles within the network for eRecognition), service (party in accordance with the Appointments System eRecognition electronic services) and users (party who accordance with the Appointments System eRecognition electronic services decreases). These committees advise on the content and development of the Appointments System eRecognition.

Membership of these bodies is set out in the Legal framework eRecognition v1.4. In addition, interested parties may join user groups. These have no formal control, but get this control through representation (nomination) in the above group of users in the three bodies.

In addition, System Council and Tactics Talk organizing working groups, who can advise on strategic, operational and tactical issues. Finally, interested parties who are not parties to eRecognition, through a participant or the chairman of the System Board, make a contribution based on previously published calendars and documents.

3.1.3.2 *Does making place in a manner as possible reflects the different interests?*

The decision in the three consultative takes place in the following manner, as stipulated in the decree establishing:

1. Both the System Board, as if the Operational Tactical Talk Talk decide matters by a majority of the votes cast.

2. The Chairman of the respective consultative have no vote. The observer may be present in the System Council also no voice. The other members can each have a vote.

3. In case of equality of votes, the proposal is rejected.

3.1.3.3 *Can an interested formal objection to the procedure followed?*

There is currently a formal objection procedure for stakeholders, established as part of the legal framework in the system eRecognition. Objections to the standardization process can be further inserted through a participant, or the chairman of the System Board. Because eRecognition a private organization, is finally going to court possible.

3.1.3.4 *Organises the standardization organization through regular consultations with stakeholders on development and management of the standard? (No hard condition)*

The various consultative bodies have their own cycle of meetings, as stipulated in the decree establishing:

• The System Board shall meet at least four times a year (Article 6).

• The Tactical Discussion meets monthly (Article 17).

• The Operational Consultation shall meet whenever the Chairman deems necessary to advise on the implementation of changes and releases in the Appointments System eRecognition (Article 25).

3.1.3.5 *Organises the standardization organization a public consultation before (a new version of) the standard is determined? (No hard condition)*

The agenda and the accompanying written documents of both System Council, Tactical Talk Talk and operational prior to meetings are made available to all participants, providers and users for consultation. The standardization organization organizes no broad public consultation before a new version of the standard is determined.

3.1.4 Is the standardization organization independent and sustainable?

3.1.4.1 *Is the development and management of the standard assigned to an independent non-profit standards organization?*

The standard is maintained by a management organization, which the Ministry of Economic Affairs, Agriculture and Innovation initiator. The organization that the standard eRecognition 1 September 2012 in management gets Logius, is an organization that was formed in 2006 under the name GBO.Overheid.

3.1.4.2 *Is the financing of the development and maintenance of the standard for at least three years guaranteed?*

For Logius there until 2014 budget earmarked for the development and maintenance of the standard. The Ministry of EL & I stands surety for funding. Financing is a year specified on the basis of plans of the management organization.

The expert believes that independence and sustainability of the standardization organization are sufficiently insured.

3.1.5 Is the (version) management standard well organized?

3.1.5.1 Does the standardization organization published policy on version of the standard? (Inter alia with regard to migration of users)

The version of the standard is set out in the Operational Manual Appointments System eRecognition. There is a biannual release cycle proposed for both the standard and the whole system. With an RFC will from version v1.5 of the standard semi-annual release cycle included in the proceedings with reference to a possible emergency procedure.

The expert suggests that this version adopted policies in addition to the existing documentation for version 1.4 of the standard to publish this creates further clarity towards users of the standard.

3.1.5.2 Is the standardization process of the standardization organization so well organized that the Forum can refrain from further scrutiny by the notification of a new version of the standard?

(This is the case if the standardization organization excellent scores in the previous sub-questions)

Before the standardization process sufficiently well controlled, it must, in the opinion of the experts that three conditions are met:

• The rules applicable in respect of intellectual property (trademark and) should be raised and should supplement the current documentation of the standard are published.

3.1.6 Conclusion

The documentation is available after registration, the decision procedure is sufficiently accessible, there is an appeals procedure and the standardization organization is independent and sustainable. The standard conforms to the opinion of the expert, however, only to the openness criteria as well as the following condition is met:

• The rules applicable in respect of intellectual property (trademark and) should be raised and should supplement the current documentation of the standard are published.

The expert advises the management organization eRecognition additionally provide:

• Publication of the version adopted policies in addition to the documentation of the standard.

• Provide insight into the changes to the standard in the different versions of documentation.

• Public availability of the documentation of the standard without notification process.

3.2 Added value

The interoperability profits and other benefits of adoption of the standard government-wide roads and public against the risks and disadvantages.

3.2.1 Is the application and scope of the notification properly defined?

3.2.1.1 Is the functional scope is well defined?

Within the chapter 2 proposed scope of eRecognition functionality is selected in the practice of the standard fully supported and already applied. In the opinion of the expert, there are no functions in this scope appointed to the standard does not support.

3.2.1.2 Is the organizational scope is well defined?

In Chapter 2 proposed organizational scope includes the opinion of the expert any relevant parties to whom the standard applies can be explained within the scope of the list of open standards for "comply or explain".

3.2.1.3 Is the standard application of the generic and not intended for data exchange with one or a limited number of specific provisions?

The default eRecognition public interface is generically applicable to all overheidswebdiensten. The default value is great for achieving interoperability within the Appointments System eRecognition, but also has added value beyond. It derives thereby added to the profile of SAML.

3.2.2 Compares the standard itself well to other standards?

3.2.2.1 Can the standard addition or in combination with pre-recorded standards are applied (ie, the standard does not conflict with already listed standards)?

The proposed scope partly overlaps with the scope of SAML, which is also on the list of "comply or explain" state. The scope of SAML is defined by:

"Federated (Web) browser-based single sign-on (SSO) and single-sign-off. This means that once a user after login via the browser to access different services from different parties."

eRecognition is a specific application (profile) of SAML.

Where SAML itself rather focuses on the following single login to access different services from different parties (SSO), the public interface eRecognition focuses on basic access service. The overlap is thereby in providing access to services on the basis of authentication data.

Based on the above, the expert group recommends that the management organization of eRecognition to, the application of both standards ironed coherence.

Does the notified default value already set up standards with overlapping functional scope and organizational scope? (This can also be a new version of the same standard go.)

The default eRecognition public interface provides a profile of the SAML v2.0 standard, with a number of choices made regarding use of the latter standard. These choices eRecognition thus limiting the freedom of choice for the SAML defined scope. Solutions that meet eRecognition are better interoperate with one another, where non-standard use of SAML v2.0 can lead to non-interoperable and customization choices between parties.

3.2.2.2 *Does the notified standard value over existing competing standards that could be eligible for inclusion? (Explanatory question)*

Potentially competing standards and solutions for standard eRecognition public interface are:

- Not standardized solutions of a public service

The added value of eRecognition is located in the standardization on an interface within eRecognition, making the problem of the diversity of authentication devices is reduced.

- Authentication based on PKIoverheid certificates (PKI)

The added value of eRecognition is located in the greater simplicity in use. In addition, PKI as a solution for the reliability levels for authentication to work as an authentication tool within eRecognition, there is talk of compatibility (confidence level 4).

- A Select Standard DigiD

The added value of eRecognition lies in the fact that eRecognition relies on an international standard (SAML), which also appear on the list of "comply or explain" state. In addition, A-Select is currently being phased out.

Standards, that affect the scope of the standard and are referred to in the discussion of the expert, are the following:

- XACML

XACML, an abbreviation for "eXtensible Access Control Markup Language", makes it possible to achieve a very deep level of detail the authorization of users and systems to define and enforce. The expert who has examined WS-Policy and XACML, has already indicated that XACML for authorization purposes in addition to the SAML could be deployed. The public interface eRecognition makes no use of XACML.

- OAuth

A standard specifies that an authorization framework, which makes it possible that third-party applications to access web services and resources. The use of OAuth is rather located in the consumer domain and the individual user and much less in the business domain. A popular standard for granting access to applications in the consumer domain, which is based on the OAuth 2.0 standard, is OpenID Connect.

- STORK

A European project in which a framework of a system of levels of reliability is developed. For interoperability within the European Union relies on the network for eRecognition its terminology and processes for confidence levels on the STORK framework.

3.2.2.3 *Is the standard an international standard or connect the standard with relevant international standards? (Explanatory question)*

The default eRecognition public interface is not an international standard, but provides a profile on top of the (international) SAML v2.0 standard.

3.2.2.4 *Does the standard of interoperability with sufficient without additional standardization agreements (such as local profiles) necessary? (Explanatory question)*

The eRecognition public interface provides a technical specification for interoperability based on a SAML profile. In the expert recommendation for SAML v2.0 is determined that additional appointments interoperability of SAML further. In the public interface eRecognition is precisely a number of choices which make up such arrangements. A number of additional agreements is still necessary to correct and interoperable use of eRecognition public interface protection. The additional appointments as are necessary to correct and interoperable use of the interface in practice to ensure interoperability and support are laid down in the agreements eRecognition system. The agreement describes the system requirements for semantic interoperability, legal and organizational fields.

In the opinion of the expert contributes to improving the standard of interoperability, precisely because it interprets some choice freedoms by use of SAML exist.

3.2.3 Are the quantitative and qualitative benefits of adoption of the standard, for the (semi-) government as a whole and for society, against the disadvantages?

3.2.3.1 *Does the adoption of the standard to the solution of an existing, relevant interoperability problem?*

The government eRecognition interface approach the problem of the diversity of authentication interfaces for separate administrations to solve ("keys"). These are government services are faced with many choices and non-standardized consistency between the technical interfaces. Companies and other organizations can eRecognition with multiple service visit and have thereby no longer any task other means of authentication required. The service provider in turn knows by eRecognition with which the service consumer (business) it does business and whether the person is authorized to act on behalf service consumer to do business with the provider.

At the same time, the expert notes that the government eRecognition interface contributes to further solve the interoperability problem on authentication. In the expert recommendation for SAML v2.0 has also been determined that additional arrangements such as those for the public interface are made, the interoperability of SAML further. Because eRecognition a SAML profile, not all existing SAML implementations are interoperable with the eRecognition interface: this is inherent in the use of SAML.

The deployment of eRecognition may in the opinion of the expert also be seen as a step towards further integration of authentication services for government services for society as a whole (both citizens and businesses). The use of DigiD in the civilian domain legitimizes although other choices regarding SAML but (also) consistency in a number of technical choices would in the opinion of the expert and the relationship between DigiD eRecognition can increase.

3.2.3.2 *Does the standard to the prevention of vendor lock-in (supplier dependency)?*

Because eRecognition provides an interface by which multiple parties can provide authentication services, government service as a user can easily switch to another party. This will avoid vendor lock-in.

Although the providers of this interface is currently mainly Dutch companies come, there is no obstacle for foreign companies to interface to deploy (or participant in the whole system).

3.2.3.3 *Weighing the government-wide and social benefits for the information and the operations against the costs?*

For the various social sectors are income and expenses as follows to characterize the public interface eRecognition:

- Public sector (service providers): the cost to government organizations are in connection costs (the interface), subscription fees at a eRecognition Broker for transaction processing and the costs that have to be made to the service behind eRecognition (digital) unlock (eg in the form of development of digital access and transaction capabilities instead of paper). In the form of avoided cost benefits will act as savings in investments for various interfaces and savings on purchase and manage multiple authentication means.
- Companies: companies find cost because they are forced to authentication resources to purchase to the interface (and the electronic services) to make use. Also an annual fee paid for use of these resources. The expectation is that companies represent an administrative burden will experience by switching from paper to digital transactions and the use of a key.
- Citizens: eRecognition is not for use by citizens of application (for non-business purposes).

A cost benefit analysis conducted for the entire system eRecognition appointments by Ecorys in 2011, shows that the proposed time horizon (2011-2015), the benefits far exceed the costs (tens of millions).

Besides the monetised benefits are also non-monetary benefits are recognized:

- Increase Business to Business (B2B) activities
- Increase Government to Government (G2G) activities
- Improve reliability through higher confidence level.

The main costs are included in the proposed period of administration (twice the introduction costs). The main (quantified) benefits from the introduction of eRecognition cover the administrative burden for companies and avoided costs and

efficiencies in government service. Because a standard comes in the form of eRecognition development and management will also decrease (avoided costs).

In the opinion of the expert roads thus the benefits against the costs.

3.2.3.4 *Are the security risks to government-wide adoption of the standard acceptable?*

In a study of safety eRecognition commissioned by the Ministry of EL & I, it was stated that the operation of eRecognition a "necessary trust 'must exist, that' stringent demands on the safety availability (data) integrity and confidentiality 'sets . If one of these aspects is compromised, or appears to be, the image of the service be seriously damaged.

The eRecognition interface (and the appointments system) have been prepared under the ICT security guidelines for web applications of NCSC, to guide the development, management and supply of eRecognition and associated infrastructure. Also in development of the interface (and the entire appointments system) requirements from the National Security Baseline (BIR) included in the risk analysis and the standards framework.

Within the system, appointments are for further use of the interface clear guidelines and process descriptions for incident management in the area of confidentiality and / or integrity (operating manual) available.

The default eRecognition public interface relies moreover on a security, which

- use is made of asymmetric encryption, on the basis of a PKI
- at least 2048 bit key lengths are enforced
- minimum SHA256 hashing algorithm is used as
- measures are taken against replay attacks
- reports / statements perishable

The expert believes that thereby the security risks for the government eRecognition interface acceptable.

3.2.3.5 Are the privacy risks to government-wide adoption of the standard acceptable?

Privacy lies in the design of the standard decided. The requirements relating to privacy are defined in the standard, and even more so, in the appointments system. eRecognition protects the privacy due to authentication companies the personal information of the authorized only within the network can be controlled and not be provided to the receiving body (public service). Only - not privacy sensitive - identification of a company and a pseudonym of the agent are provided.

With demonstrable fraud presumption by a procedure the identity behind a pseudonym be obtained from eRecognition party. A user of the service can also choose his identity after login to the service provider to disclose, for example, by imparting name or email address in the attributes.

3.2.4 Conclusion

The expert believes that the benefits of government eRecognition interface outweigh the risks and disadvantages.

The government-wide and societal benefits outweigh the costs, and privacy and security risks in the standard is sufficiently covered. The standard also provides added value compared to the standard SAML v2.0. The advantages of the standard public interface eRecognition are particularly reflected in the reduction of the diversity of authentication features and the contribution it makes to reducing interoperability problems in this area. The interface is also an independent top SAML profile also turn off the system to eRecognition.

There are alternatives to the standard, but these are less easy to use, be phased out or know much lesser extent, embedding into an elaboration of rules and agreements (such as the appointments system eRecognition) to correct and interoperable use of the standard guarantee.

3.3 Support

Providers and users must have sufficient experience in supporting, implementing and using the standard.

3.3.1 Is there sufficient market support for the standard?

3.3.1.1 Provide multiple vendors support the standard?

At the time of writing there are 6 accredited providers who fulfill the role of eRecognition Broker and eRecognition public interface offer: KPN, Gemnet, Connectis, iWelcome, CreAim and Digidentity.

3.3.1.2 *Can a user the conformity of the implementation of the standard (let) buttons?*

Testing and monitoring of service is described in the documentation of the appointment system. To support the management organization manages an online facility for these tests to be carried out. The conformance test is performed in the system through a eRecognition testing tool for service, an instrument messages and the answers to assess conformance to all appointments system. Besides this facility offer the players who fill the broker also testing facilities (on a commercial basis).

3.3.2 Can the default count on sufficient support?

3.3.2.1 *If the notified version of the standard within the organizational scope used by multiple organizations?*

At the time of writing there are 40 public service connected jointly offer 44 different e-services using eRecognition. This concerns both rural (including Message Box for Answers for Businesses, Ministry of Infrastructure and Environment, Ministry of EL & I, IND) and local authorities (eg Rotterdam, Zwolle city, municipality of Zoetermeer).

Furthermore, a number of governments in preparation for implementation of eRecognition including OPTA, CJIB, IVW and province of Groningen.

3.3.3 If a previous version of the standard within the organizational scope used by multiple organizations?

At the time of writing in all government organizations have an older version of the public interface eRecognition in use (version 1.1). It is expected that by the end of 2012 version 1.4 implemented and supported by the relevant parties.

The (mandatory) technical differences between versions 1.1 and 1.4 versions are limited to

- Entry of new Chamber office numbers
- Required time synchronization
- Mandatory use G2 SSL certificates

For eRecognition public interface is that the public service is allowed to use older versions. A broker is only required current, current version of the interface and make the version support (N/N-1-principe for management of versions in the lifecycle of the interface). A broker can also choose not to support older versions: there is no final term.

3.3.3.1 *Is the notified version backward compatible with earlier versions of the standard?*

The registered version of the standard provides enhancements over the previous version (s) of the interface standard. The current version of the interface is backward compatible with previous versions, except that new functionality is not available for users who have an earlier version implemented.

Are there sufficient positive signals about future use of the standard by (semi-) government organizations, businesses and citizens?

The number of users and affiliated service has increased over the past year and is still growing.

In iNUP further states that all municipalities have the obligation eRecognition as NUP module to implement, as part of Operation NUP. The Digital Agenda.nl eRecognition is also called as authentication agent (linked to an authorization agent) in the context of the policy theme to make it possible for companies to do

business electronically with the government ("right of e-business for companies").

There may be a caveat be placed at the current difference between authentication services in civil and business domain. For companies domain eRecognition the developed solution for the civilian domain is DigiD. The A3-report describes that it is desirable for these two domains on the time to grow towards each other.

3.3.4 Conclusion

The expert believes that there is sufficient support for the standard, there is support for the market standard by multiple vendors, and there is policy support for eRecognition in iNUP and Digital Agenda.nl. The number of affiliated providers of public services at the time of writing about 40 (44 administrations) and increases in number.

3.4 Recording promotes adoption

The inclusion on the list is a suitable means to the adoption of the standard of.

There are two lists: the list of common standards and the list of 'comply or explain'. The latter list is intended to standards an additional incentive if:

1. Their adoption within the current (semi-) government is limited;

2. Recording contributes to the adoption by stimulating obv the 'comply or explain' regime.

The list of common standards is a reference for standards that are commonly used. If standards meet some basic conditions (for eg openness), there is no discussion and standards are widely used, it will be included on that list instead.

Placement on the 'comply or explain' list confirms the government developed and implemented policies to achieve a rural herkennings-/authenticatiedienst. An obligation through 'comply or explain' sees the expert also as a means of iNUP and Digital Agenda made policy goals and administrative arrangements actually achieve and the use of the eRecognition standard practice to promote.

For inclusion in the list there is some overlap with the standard SAML already on the 'comply or explain' list. Recommendation of the expert to the Forum:

- To pay attention to the relationship between standards in the field of identification, authentication and authorization and to examine how these two standards relate to each other in a framework for this domain.

A recommendation that the expert does the management organization for eRecognition is:

- examine how the application of SAML and public interface eRecognition can be better coordinated and, where necessary, a proposal for an alternative definition.

A recommendation that the expert does Logius and eRecognition jointly:

- to ensure consistency (and in particular the consistency in a number of technical choices) between DigiD and eRecognition mapping and where possible improve.

Placement on the 'comply or explain' list confirms the government developed and implemented policies to achieve a rural herkennings-/authenticatiedienst. An obligation through 'comply or explain' sees the expert also as a means of

iNUP and Digital Agenda made policy goals and administrative arrangements actually achieve and the use of the eRecognition standard practice to promote.

For inclusion in the list there is some overlap with the standard SAML already on the 'comply or explain' list. Recommendation of the expert to the Forum:

- To pay attention to the relationship between standards in the field of identification, authentication and authorization and to examine how these two standards relate to each other in a framework for this domain.

A recommendation that the expert does the management organization for eRecognition is:

- examine how the application of SAML and public interface eRecognition can be better coordinated and, where necessary, a proposal for an alternative definition.

A recommendation that the expert does Logius and eRecognition jointly:

- to ensure consistency (and in particular the consistency in a number of technical choices) between DigiD and eRecognition mapping and where possible improve.

4 Opinion of Forum and Board

4.1 Summary of assessment criteria

In summary, the opinion of the expert group on the assessment criteria as follows:

4.1.1 Open standardization process

The documentation is available after registration, the decision procedure is sufficiently accessible, there is an appeals procedure and the standardization organization is independent and sustainable. The standard conforms to the opinion of the expert, however, only to the openness criteria as well as the following condition is met:

• The rules applicable in respect of intellectual property (trademark and) should be raised and should supplement the current documentation of the standard are published.

4.1.2 Added value

The expert believes that the benefits of government eRecognition interface outweigh the risks and disadvantages.

The government-wide and societal benefits outweigh the costs, and privacy and security risks in the standard is sufficiently covered. The standard also provides added value compared to the standard SAML v2.0. The advantages of the standard public interface eRecognition are particularly reflected in the reduction of the diversity of authentication features and the contribution it makes to reducing interoperability problems in this area. The interface is also an independent top SAML profile also turn off the system to eRecognition.

There are alternatives to the standard, but these are less easy to use, be phased out or know much lesser extent, embedding into an elaboration of rules and agreements (such as the appointments system eRecognition) to correct and interoperable use of the standard guarantee.

4.1.3 Support

The expert believes that there is sufficient support for the standard, there is support for the market standard by multiple vendors, and there is policy support for eRecognition in iNUP and Digital Agenda.nl. The number of affiliated providers of public services at the time of writing about 40 (44 administrations) and increases in number.

4.1.4 Recording promotes adoption

Placement on the 'comply or explain' list confirms the government developed and implemented policies to achieve a rural herkennings-/authenticatiedienst. An obligation through 'comply or explain' sees the expert also as a means of iNUP and Digital Agenda made policy goals and administrative arrangements actually achieve and the use of the eRecognition standard practice to promote.

For inclusion in the list there is some overlap with the standard SAML already on the 'comply or explain' list. Recommendation of the expert to the Forum:

• To pay attention to the relationship between standards in the field of identification, authentication and authorization and to examine how these two standards relate to each other in a framework for this domain.

A recommendation that the expert does the management organization for eRecognition is:

• examine how the application of SAML and public interface eRecognition can be better coordinated and, where necessary, a proposal for an alternative definition.

A recommendation that the expert does Logius and eRecognition jointly:

• to ensure consistency (and in particular the consistency in a number of technical choices) between DigiD and eRecognition mapping and where possible improve.

4.2 Advice to Forum and Board

The expert advises majority government standard interface eRecognition, version 1.4, to include on the list of 'comply or explain' if the following conditions are met:

• Mention and publish the provisions regarding intellectual property in addition to the documentation of the standard.

With the scope:

"Authentication for Web services of public services to businesses and organizations and to establish the authority of the requested service."

And if scope:

"Governments (central government, provinces, municipalities and water boards) and institutions in the (semi-) public sector."

At the time of writing, speaking three parties, namely the Tax Logius and the Ministry of the Interior is not yet on inclusion in the list.

4.3 Recommendations with respect to the adoption of the standard

For inclusion in the list there is some overlap with the standard SAML already on the 'comply or explain' list. Recommendation of the expert to the Forum:

• To pay attention to the relationship between standards in the field of identification, authentication and authorization and to examine how these two standards relate to each other in a framework for this domain.

A recommendation that the expert does the management organization for eRecognition is:

• examine how the application of SAML and public interface eRecognition can be better coordinated and, where necessary, a proposal for an alternative definition.

A recommendation that the expert does Logius and eRecognition jointly:

• to ensure consistency (and in particular the consistency in a number of technical choices) between DigiD and eRecognition mapping and where possible improve.

5 References

[1] Action Plan Netherlands in Open Connection, The Hague: Ministry of Economic Affairs, 2007.

[2] "Comply or explain" is defined in the "Instruction civil service when purchasing ICT services or ICT products" of 8 November 2008, and also in covenants and agreements with local authorities. See: http://www.open-standaarden.nl/open-standaarden/het-pas-toe-of-leg-uit-principe/

[3] "Decree establishing the College and Standardisation Forum 2010". See: https://zoek.officielebekendmakingen.nl/stcrt-2010-4499.html

[4] Criteria and procedure for 'comply or explain', adopted by the

Standardisation Board on 23 June 2011. See: http://www.forumstandaardisatie.nl/fileadmin/os/images/Toetsingsprocedure_en_criteria_v1__0.pdf