De Werkmaatschappij
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Market Consultation

Haagse Inkoop Samenwerking (HIS)

Visiting address
Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

eID Resource

on behalf of the

Ministry of the Interior and Kingdom Relations

Contact person	Henk Strik
Date	8 July 2013
Ref. Nr.	201300114.052.004
Version	1.0
Status	Final

Table of Contents

Abbreviations and definitions

Authentication	Establishment that the person requesting access is actually the person who he/she claims to be.
Authentication service	Its purpose is to permit a user to access multiple applications while providing their credentials
Authorisation	Establishment that the person requesting access is actually authorised for that access.
BIG registration	Registration in the BIG Register. The BIG register is a task dictated by the BIG Act (*'Wet op de Beroepen in de Individuele Gezondheidszorg'*, the Individual Healthcare Professions Act). The BIG register provides clarity about the authority of a care provider.
BSN	Citizen Service Number. Unique personal number for everyone registered in the municipal personal records database (GBA). See also http://www.bprbzk.nl/BSN/Wat_is_het_burgerservicenummer_BSN
IKR	Ministry of the Interior and Kingdom Relations.
Certificate	An electronic document (data structure) that contains a public key digitally signed by a known authority (Certificate Authority), which guarantees that the public key is linked to the owner of the electronic document.
DigiD	Username and password (in combination with SMS text message) for identification on government web sites. See also https://www.digid.nl/
DigiD card	Smartcard with contactless chip, with an eID supplementing the DigiD.
ECC	European Citizen Card.
eID	Electronic identity that can serve as electronic form of personal identification. Usually takes the form of an applet on a chip.
eID system	System that ensures that citizens can electronically identify themselves when they interact online with the government, the private sector or other citizens.
eHerkenning	System that ensures that companies can electronically identify themselves when they interact online with the government or other companies. See also http://www.eherkenning.nl/
Enisa	European Network and Information Security Agency. See also http://www.enisa.europa.eu/about-enisa
Photomatrix 2007	Criteria that the passport photo on identity documents must meet. See also http://www.bprbzk.nl/content.jsp?objectid=BPRextern:5126

GBA	Municipal Personal Records Database (*Gemeentelijke Basis Administratie persoonsgegevens*). See also http://www.bprbzk.nl/GBA
Semi-manufactured card	A card in credit card format with a design and a chip that is not yet personalised.
Hotspot	Hubs in the electronic infrastructure through which electronic footprints can be traced, by means of which profiles of persons and activity can be created (i.e., from whom has a citizen procured services electronically, and what services).
IRMA	'I Reveal My Attributes'; project for safely providing attributes. See also: https://www.irmacard.org/
NFC	Near Field Communication
NIK	Dutch Identity Card. See also http://www.paspoortinformatie.nl/nederlands/Reisdocumenten/Nederlandse_identiteitskaart
OTP	One-Time password
PC	Personal Computer
PKI	Public Key Infrastructure. System for use and management of certificates.
Privacy	The right of a natural person, when conducting personal activities, to determine the extent to which he/she interacts with the environment, including the extent to which the person is willing to share information about himself/herself with others.
Pseudo-id	To protect the privacy, not the BSN is showed, but a pseudonym.
PUK	PIN Unlock Key, also known as the personal unlock key.
QES	Qualified Electronic Signature
Service Provider	A company that provides organizations with the service they want to deliver.
STORK	Secure idenTity acrOss boRders linKed. European framework programme for the exchange of electronic identities between the member states. The STORK project features authentication levels from 1 through 4.
User	Person that uses a public service.
WBP	The Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*).
WID	The Compulsory Identification Act (Wet op de identificatieplicht). Section 1 lists the documents designated as identification documents.

1 Introduction

1.1 Background for market consultation

The Ministry of the Interior and Kingdom Relations (hereinafter IKR) has defined social living in a democratic state under the rule of law as a key focus area. Important topics within its responsibility are the electoral system, travel documents and domestic governance. Within IKR, the Directorate of Citizenship & Information Policy (C&I) is the directorate primarily engaged with the relationship between the government and society. An important part of this is the digitisation of society and the way in which the citizen can access electronic services. The authentication resources we know today will not be adequate in the future. There is an increasing need in society for a higher level of authentication resource (STORK 4) for procuring electronic services.

In the summer of 2012, IKR conducted a strategic survey to explore the potential for a system of electronic identity (eID). Based on the results, two tracks were identified.

- Track I is the creation of an eID system in the Netherlands.
- Track II is the creation of scenarios for an eID resource for the citizen with a high degree of reliability.

In order to be able to make an informed decision on a new eID resource, we are conducting a market consultation for Track II. The choice was made for a Public Request for Information (RFI). The actual introduction of an eID system and corresponding resource will depend on parliamentary decision-making.

1.2 Objective and scope

This market consultation focuses on delivering a new resource for authentication and identification in the procurement of electronic services. In addition, there must be a capacity to load additional attributes on the chip or to place an electronic signature after issue of the resource.

The object of the market consultation can be described as follows:

1. IKR has been investigating the introduction of an eID for some time. Now that plans are becoming more concrete, IKR wishes to inform the potential market parties officially and uniformly of the plans for the eventual introduction of an eID system and a new eID document.
2. Experts have formulated required conditions. IKR wishes to review these conditions for feasibility and effectiveness. Additionally, IKR wishes to be able to make a realistic assessment of the potential costs of an eID resource. The information obtained will be used in the preparation for decision-making on the eventual introduction of an eID system and the tendering procedure if that option is chosen.
3. To obtain a good picture of the existing, proven solutions available in the market.

1.3 Outline

This document begins with the conditions a participant in this RFI must meet, followed by the timeline. Chapter 3 describes the background for an eID system. Chapter 4 details the key requirements. The questionnaire is provided in chapter 5.

The questions are broken down into a number of subject areas:

1. Organisational details
2. General
3. Required conditions
4. Technology
5. Solution
6. eID system

2 Conditions for participation in market consultation

A number of procedural conditions are attached to this market consultation. These conditions are identified and explained below.

2.1 Consent

Your participation in this market consultation entails that you consent to the terms of these conditions.

2.2 Objective of conditions

The objective of these conditions is to ensure that we receive the information in such a way as to be able to process them effectively.

2.3 Objective of market consultation

IKR will decide what requirements and/or wishes it will stipulate in any tendering procedure it may hold after the market consultation, in observance of applicable law. The Ministry is not obliged to draft requirements and/or wishes in the ultimate tendering process such that each party that participated in the market consultation will be able to meet the requirements.

2.4 Public consultation

This market consultation is a public consultation, in the sense that it is being announced publicly. Any market party that so desires may participate in the market consultation. If a party has a sub-solution, only the questions pertaining to this solution need to be answered.

2.5 No request for quotes

This market consultation is explicitly not a request for quotes. No rights can be derived from this consultation.

2.6 Use of information

IKR will use the information obtained in the context of this market consultation for preparing the decision-making on the ultimate introduction of an eID, decision-making on any tendering process to be used, and for the preparation and presentation to the market of this tendering process.

2.7 Contact person

During the market consultation, a single contact person will act on behalf of the Contracting Authority. That contact person is: **H.M. Strik, Senior Procurement Consultant HIS.**

All communication concerning this tendering procedure will go through CTM and be addressed to the contact person for the Contracting Authority. Participants may not approach other officials of the Contracting Authority directly or in any other manner.

2.8 HIS: The Hague Procurement Cooperative

In conducting this market consultation IKR is assisted by the Haagse Inkoopsamenwerking (hereinafter HIS). The HIS is a procurement office initiated by the ministries of:

- Internal Affairs and Kingdom Relations (IKR)
- Foreign Affairs (FA)
- Finance (FIN) and Public Health
- Social Affairs & Employment (SAE)
- Welfare & Sport (W&S)

As a business unit, HIS falls under the Delivery Agency (DWM), under the Directorate-General of Organisation and Operations of the Kingdom (DGOBR) of the Ministry of the Interior and Kingdom Relations.

2.9 CTM solution tendering tool

To organize this RFI the contracting authority has chosen the platform of Complete Tender Management (CTM), provided by EU-Supply.
By using the CTM platform the HIS is able to execute all tenders and contracts efficiently, completely and electronically.

The CTM platform has been used for conducting online tenders since 1999 and is now being used in used in 11 countries within the European Union. Within a number of these countries CTM is chosen as the National platform for tendering.

CTM is ISO 27001 compliant; this ISO norm is a standard for information security.
This norm specifies demands for defining, implementation, executing, checking, evaluating, keep up-to-date, and improving a documented Information Security Management System (ISMS) scoping general company risks. For more information, please refer to: www.ctmsolution.nl.

If you, as a supplier, experience any technical difficulties when using CTM (for example if you are unable to login) then please don't hesitate to contact the CTM support desk:

- Telephone: +31 (0)20 - 670 8500(9 am - 6 pm)
- E-mail: helpdesk@ctmsolution.nl

You are also able to download the CTM supplier manual, which describes the most relevant actions in relation with providing an offer and communication.
You can find this manual attached, or available as a download from the CTM homepage (after logging in).

If you are interested in competing within this tender, please start by registering your company for access with a unique ID:
https://eu.eu-supply.com/login.asp?B=CTMSOLUTION&target=&timeout=
All requests and communication for further information relevant to content and procedural aspects regarding this tender will also be handled using CTM.
Within the specific tender on CTM you can select the menu item 'Messaging'.

2.10 Format in which response should be supplied

Your response should preferably be supplied in MS-Office and PDF format.

2.11 Language in which data must be supplied

The working language for this consultation is English. The documents are drafted in the English language. Questions from market parties must be submitted in English.

Market parties may also submit their responses to the questions of chapter 5 in Dutch.

2.12 Reference

On all communication, please reference: 'Market consultation eID resource'.

2.13 Questions

All supplier questions concerning this market consultation must be submitted exclusively to **H.M. Strik, Senior Procurement Consultant HIS.**

2.14 Problems in tendering documents

In the event of any contradictions/problems in the documents, please inform HIS.

2.15 No expense reimbursement

No participants in the RFI will be reimbursed for expenses incurred in the participation in this market consultation under any circumstances.

2.16 Publication date

This market consultation has been sent for publication on July 8th 2013 to TenderNed and the Tender European Daily (TED), the publication medium for government contracts falling under EU Directive 2004/18.

2.17 Closing of response period

The term within which responses to the questions will be accepted ends on August 2nd 2013 Submissions received after this date will not be accepted.

2.18 Further questions

If responses from market parties give IKR reason to do so, the Ministry may invite these parties to explain their responses individually by means of a demonstration. Any such demonstrations will take place in weeks 34 and 35.
Where it deems necessary, the Ministry will contact any such relevant market parties in due course.

2.19 Reporting

After completion of the consultation, the responses will be compiled into a report. This report will be made available via HIS.

2.20 Timeline (indicative)

The intended timeline for the market consultations is as follows (the Ministry reserves the right to make changes to this timeline):

Activity	**Date**
Publication of market consultation	8 July 2013
Closing of response period	2 August 2013
Where responses from the market give reason to do so: individual information sessions by a limited number of invitee market parties	Weeks 34 and 35
Forwarding of report to participants	1 October 2013

3 Background information

In order to properly be able to answer the questions in this consultation, you need to be aware of the background to these questions. This chapter first describes a general outline and subsequently addresses the scenario that IKR envisions.

3.1 Move to electronic communication

Dutch society is digitising fast. Electronic services are user-friendly, efficient and cost-effective. For the private and public sectors, confidence in electronic services is essential. In order to guarantee this confidence, the current reliability of existing electronic identification resources (username/password) must be taken to a higher level. There is now an eHerkenning system for companies in place. This system allows companies to electronically identify themselves when they interact online with the government or companies. At present, individuals do not have an equivalent system available for electronic interaction. There is a need for resources on a wide scale to facilitate electronic authentication for citizens at higher levels of security.
The underlying assumptions here are:

- For individuals and companies, the use of reliable authentication resources and electronic services in the future has to be safe
- Easy-to-use (anytime, anywhere)
- Privacy must be adequately guaranteed.
- The intention is to release multiple public and private resources.
- The resource will span the boundary of the distinction between citizens and organisations. For a large group (approximately 1.1 million) of natural persons who have a company in certain legal forms (such as sole proprietorship), a distinction between resources for individuals and companies would be undesired.

3.2 A strong electronic identity for the citizen

The goal is to make a high-level (STORK 3 and 4) eID resource available to citizens. Companies already have one available in eHerkenning.
The new eID resource would be both a public and a private resource:

- For public resources (level 4), this refers to the placement of an eID on a government document.
- In reference to private resources, this means making broadly rolled out resources (e.g. bank resources) suitable for government services, as well as the set up of a number conversion facility for use within the public domain.
- Parallel to this process, innovations in other eID resources (such as that of mobile devices) will be followed. These resources could be used as seen fit according to developing views.

The use of this eID resource sets high standards on guaranteeing user privacy.

3.3 Smartcard

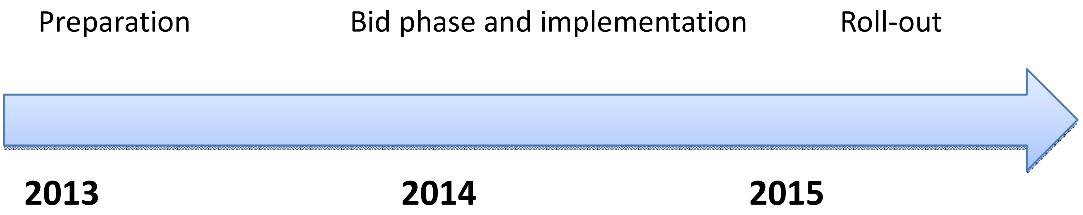
3.3.1 scenario

The preferred scenario is one in which the eID application is used on a newly introduced card. This new card, the so-called 'DigiD card', is equipped with a contactless chip and has a security level of STORK 4. The eID will record a limited number of fixed, predetermined attributes. The reason for introducing a smartcard is that IKR has a preference for introducing an eID resource that is not carrier/device-specific. In the future, the eID must also be able to be placed on other devices such as smart phones, bank cards, etc. This will give the citizen the choice of which device to use the eID with. Another reason for the choice of a smartcard is that this technology has proven itself in practice. A smartcard also meets the requirement that the user must maintain physical control over the resource on which the key is present, in order to authenticate himself/herself at a high (STORK 4) level.

3.3.2 Timeline

The expectation is that the initial rollout will be 10 million cards over three years. Thereafter, new cards will be needed for replacements and for new applicants.

The timeline for implementation of this scenario is as follows:



The timeline depends on the political decision-making. The expectation is that after summer 2013 a decision will be made on the introduction of an eID system.

3.3.3 Semi-manufactured card with chip

IKR is considering purchasing a semi-manufactured card made of polycarbonate with a simple security design. .

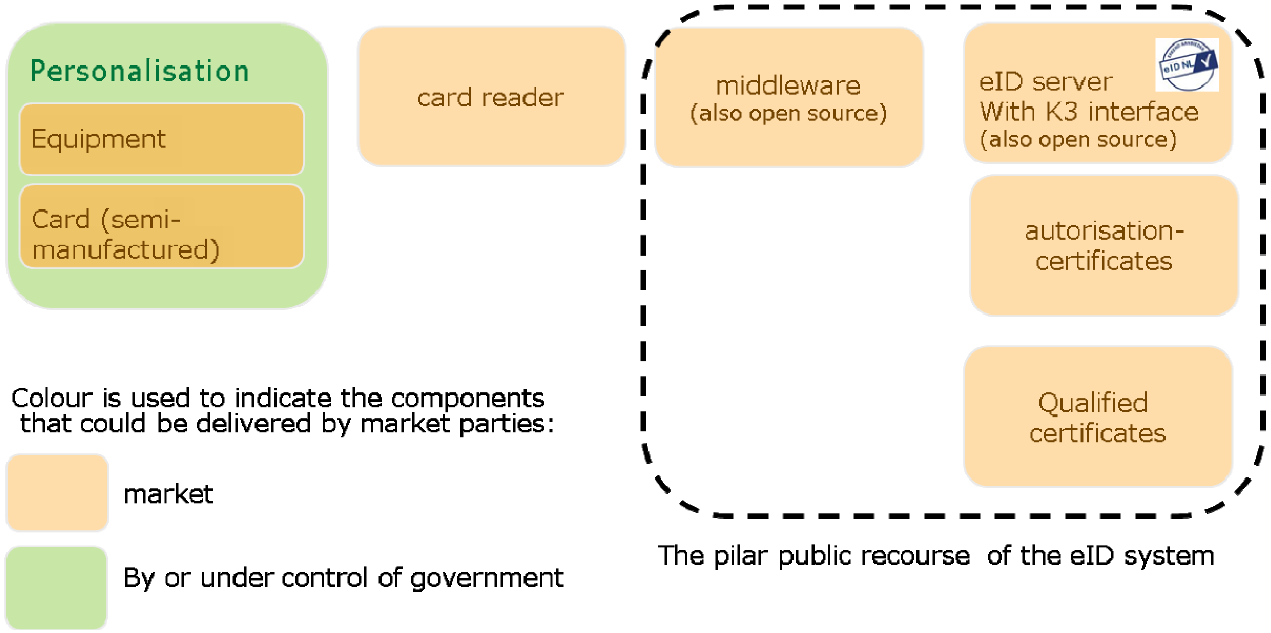
The following numbers are expected:

Year after introduction:	Number of cards
1st year	4 million
2nd year	3 million
3rd year	3 million
4th year	200,000
5th year	200,000

The semi-manufactured card must be equipped with a contactless chip and an eID application.

3.3.4 Personalisation and distribution

Depending on the results of this consultation and the outcome of parliamentary decision-making, the personalisation of the DigiD card could be handled by the government itself. The same goes for the delivery of the personalised cards at issue points (see 3.3.6). Schematically the distribution of the different components between market and government would look as follows:


Personalisation
Equipment
Card (semi-manufactured)
card reader
middleware
(also open source)
eID server
With K3 interface
(also open source)
autorisation-certificates
Qualified certificates
Colour is used to indicate the components that could be delivered by market parties:
market
By or under control of government
The pilar public recourse of the eID system

3.3.5 Middleware

Software (middleware) is required on the PC connected to the card reader in order to have an eID communicate with functions of the eID system or third-party applications that require authentication or need to read attributes. This software is situated between the eID and the application, which is why it is sometimes referred to as 'middleware.' The installation of the software for the different combinations of equipment and versions of the operating system must be as simple as possible.
The technology must not be susceptible to PCs infected with malware. The secure exchange of sensitive data and identification must be guaranteed, even on a PC infected with malware.

3.3.6 Issue

For certain services (age verification, registration of birth, etc.) the DigiD will have to serve as a legal identity document. In order to guarantee that the card is issued to the correct person, it must be issued personally (face-to-face). Like all other legal identity documents, it must be issued at a Dutch municipality office. The municipal officials will establish the identity of a citizen in the course of the issue process.

3.3.7 Privacy

For considerations of privacy, the following components are important:

1. Pseudo-ID: There must be an option to generate pseudo-IDs with cryptographic algorithms to guarantee privacy in the private domain. The use of pseudo-IDs makes it more difficult to link registers based on a unique identification.
2. Minimal disclosure: only the data set required for the service may be provided. Consider the minimum data required for a purpose such as age verification. Rather than providing the date of birth, a confirmation that the person is older than 18 is sufficient.
3. No hotspots: no central location(s) where the data is exchanged. Direct contact with the service provider must be possible. For private parties, it may be desirable to avoid having the contact go through a third party. Other institutions would easily be able to approach that third party for the data.

3.4 eID system

The DigiD card will be a part of the eID system. For the last question in this document, you will need to have some background information about the design principles of the eID system. These will be explained below.

3.4.1 Design principles of eID system

The eID system comprises a set of standards by which functions for identification, authentication and other purposes are described in a standard manner. The following design requirements are stipulated for the functioning of the authentication process for natural persons (users):

1. Every authentication process generates a pseudo-ID for the user that meets the same conditions.
2. As a result of the authentication process, the pseudo-ID is included in a standardised authentication statement.
3. The authentication statement is implemented as a SAML message (authentication assertion) in accordance with the guidelines of the Kantara Initiative.
4. Finally, the authentication statement is signed directly or indirectly by (or in any event, under the responsibility of the) authentication service.

3.4.2 Standard flowchart with pseudo-ID

These design principles are structured to allow a service provider to focus on receiving a standardised authentication statement. This authentication statement is independent of the specific technology that an authentication service uses, and thus is independent of the specific details of the corresponding authentication resources. The functionality of the authentication process is technology-independent for the service provider.

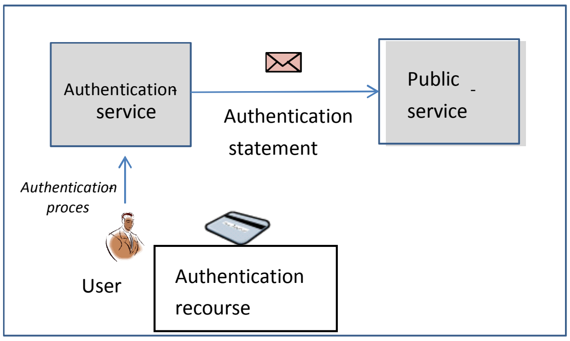


Figure 1: Standard flowchart with pseudo-ID

The flowchart shows the general pattern of an authentication process. The user has an authentication resource and uses it with the authentication service. The authentication service evaluates the successful performance of the authentication and composes the authentication statement as a SAML message. The functional content of the Identity Statement is provided in Appendix 1.

3.4.3 Standard flowchart with sector-ID

In the event that the user uses a governmental service provider, the pseudo-ID in the authentication statements is linked to the BSN of the user through a number conversion service of the government, based on a BSN linking register.

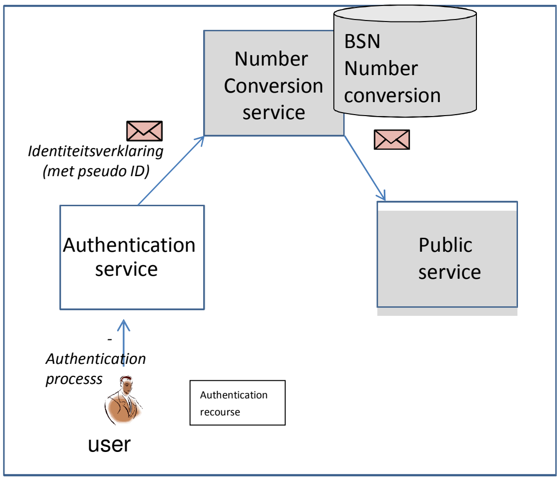


Figure 2: Flowchart with sector-ID

4 Preconditions

IKR has formulated required conditions. A number of key requirements have been established based on these required conditions. These key requirements are the basis for the new eID resource.

4.1 Key requirements

IKR distinguishes the following key requirements:

	Description
K01	The eID comes on a smartcard with a contactless chip. *The eID must be usable with a variety of peripherals. This avoids dependency on a single device, giving the citizen the choice of what device to use with his/here ID. Another reason for the choice of a smartcard is that this technology has proven itself in practice. A smartcard also meets the requirement that the user must maintain physical control over the resource on which the key is present, in order to authenticate himself/herself at a high (STORK 4) level.*
K02	No hotspots *Due to considerations of privacy, it should be possible that data exchange avoids central locations. Direct contact with the service provider must be possible. For private parties, it may be desirable to avoid having the contact go through a third party. Other institutions would be inclined to approach that third party for the use of the data.*
K03	Pseudo-IDs are generated by cryptographic algorithms *This can be used to guarantee privacy in the private domain. The use of pseudo-IDs makes it more difficult to link registers based on a unique identification.*
K04	Age verification *Only the data set required for the service may be provided. Consider the minimum data required for purpose such as age verification. Instead of providing the date of birth, a confirmation that the person is older than 18 is sufficient.*
K05	Malware The integrity and confidentiality of the data exchanged must be immune to malware infection. It must be possible to securely identify one's self and obtain services even on a PC infected with malware. See the Enisa recommendation[1]: Assume all PCs are infected.

4.2 Design decisions

	Description
B01	The government will itself issue a high-level eID to citizens. *The government has a duty of care. This means the citizen must have the option to choose a government resource.*
B02	Both the issue process and the resource itself must be qualified at level STORK-4
B03	Alongside public service providers, private service providers will be an option for the eID *The government's duty of care also encompasses guaranteeing an authentication infrastructure that can broadly support social interaction, both public and private.*
B04	Between the services infrastructure, the eID resources infrastructure and the technology used, there must be points of disconnection. *The burden on service providers should be minimized. This means the use of standard connection methods. Disconnection of technology will also make the system generally more future-proof.*
B05	eID resources must be in compliance with European Citizen Card (ECC) standard CEN TS 15480. *In order to be able to use the eID within the various countries of the EU, the resource must meet European standards and specifications.*

[1] http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps

4.3 Requirements for the eID

Alongside functional requirements (what must the eID do?), nonfunctional requirements must also be set on user-friendliness, reliability, performance and maintenance. These are often referred to as FURPS attributes. FURPS is an acronym for:

- **F**unctionality - Feature set, Capabilities, Generality, Security
- **U**sability - Human factors, Aesthetics, Consistency, Documentation
- **R**eliability - Frequency/severity of failure, Recoverability, Predictability, Accuracy, Mean time to failure
- **P**erformance - Speed, Efficiency, Resource consumption, Throughput, Response time
- **S**upportability - Testability, Extensibility, Adaptability, Maintainability, Compatibility, Configurability, Serviceability, Installability, Localizability, Portability

For every requirement, the 'import' column provides an indication of how important the requirement is and the domain it is relevant to. Here we use the MoSCoW classification:

- M - MUST: Describes a requirement that must be satisfied in the final solution for the solution to be considered a success.
- **S** - SHOULD: Represents a high-priority item that should be included in the solution if it is possible. This is often a critical requirement but one which can be satisfied in other ways if strictly necessary.
- **C** - COULD: Describes a requirement which is considered desirable but not necessary. This will be included if time and resources permit.
- **W** - WOULD: Represents a requirement that stakeholders have agreed will not be implemented in a given release, but may be considered for the future. (note: occasionally the word "Won't" is substituted for "Would" to give a clearer understanding of this choice)

Two distinct areas of use are identified for the eID: use of the resource with government service providers (G) and in the market (M). Here the 'market' also refers to use between two individuals/citizens. This is indicated in the 'area' column.

4.3.1 Requirements dictated by government

In this section, we formulate the requirements that the government has defined as necessary for application of the eID. This may also include requirements dictated by the market. Additional requirements necessary for use by private service providers are described in the following section.

Functionality

	Criteria	Import	Area	Description
F01	electronic ID	M	G	In the government domain, the eID must supply an electronic identity that is equal to or can be linked to the BSN.
F02	electronic signature	M	G/M	The eID must be capable of providing a legally valid electronic signature.
F04	user consent	S	G/M	For considerations of 'privacy by design', the WBP requires that privacy issues should be taken into account during the design phase. A user must grant explicit permission before his/her information is provided. A user may also decline to provide any critical or noncritical information, even if the result is that the service does not work. The user must have complete control here. In the government domain, the only attribute is that an identifying reference is sent that is equal to the BSN or has a one-to-one relationship with the BSN, so that the BSN can be derived.
F05	offline use	S	G/M	Certain applications of the eID must be usable offline. These are applications with lower authentication levels and generally requiring minimal disclosure. An example would be an application that requires the user's age. A date of birth does not change, and the eID can determine independently whether someone is older than 16 or 18, or younger than 65 (for example).
F10a	mutual authentication	S	G/M	Enisa has indicated that PCs and other user devices can no longer be trusted due to the rise of viruses and malware. This is a paradigm shift. If the PC can no longer be trusted, then the eID must be able to authenticate the service provider (who am I communicating with?). This means there must be mutual authentication (both systems identify themselves).
F10b	purpose limitation	S	G/M	If the PC cannot be trusted (see F10a), then trusted functionality on the eID must be able to determine what information the service provider can request, in other words, where the information is purpose-limited. This information should not be obtained from the PC, because the PC may be compromised.
F10c	Encryption or electronic signature	S	G/M	If the PC cannot be trusted (see F10a), then it is important to ensure that the communication between the eID and the service provider is secure. This requires encryption between the eID and the service provider.
F12	contactless communication	S	G/M	Growing use of mobile devices is predicted for the future, which will make contactless communication the standard. Right now, that standard is NFC (Near Field Communication). This is why the eID must have contactless communication capability. This is also a reliability requirement, because contactless chips have a longer lifetime than contact chips.
F13	Loss/theft	M	G/M	The eID must be able to be rendered unusable in the event of loss, theft or decease. A distinction can be made by function. The identification function is essential and must be revocable with immediate effect. Revocation can be dealt with more flexibly for other functions and attributes.
F14	high authentication level	M	G/M	The eID must meet the highest European standard, STORK level 4. This level is suitable for placing a legally valid electronic signature. This sets requirements on the legal framework, on the use of the technology and processes surrounding issue and management.
F15	proven technology	M	G/M	In order to minimize the risks of implementation, the eID must be based on proven technology that is secure.
F16	upgrading eID	S	G/M	The eID system must allow subsequent addition of new applications to the eID or improvement of existing ones in a secure manner. This must prevent the mass reissue of eID resources upon upgrades. Additionally, certificates with the maximum lifetime of five years must be replaceable if the lifetime of the device is longer (see R01). .
F17	European Citizen Card	S	G/M	The eID must meet the European requirements stipulated for an eID, and specifically the requirements based on the European Citizen Card.
F18	European interoperability	M	G/M	The eID must be functional across national borders (assuming that the eID is notified). The eID must be in compliance with the Electronic Trust Services Regulation (Regulation 2013/C 28/04).

Usability

	Criteria	Import	area	Description
U01	metaphor	M	G/M	The citizen has to actually use the eID. This makes user friendliness extremely important. This is the reason that Germany devoted a great deal of attention to the metaphor: how do you explain to citizens what an eID is and what it does? The metaphor Germany has chosen is: 'what's on the card is in there and, with the exception of the passport photo/signature, can be provided to the service provider after approval by the user.' The functionality of the eID should be readily explainable to the citizen.
U02	supporting OS	M	G/M	At a minimum, the following operating systems must be supported: Windows: XP, Vista, 7 and higher. Mac OS-X Lion, and higher Linux: (latest stable versions of) Ubuntu and Suse
U03	middleware	S	G/M	Software (middleware) is required on the PC connected to the card reader it in order to have an eID communicate with functions of the eID system or third-party applications that require authentication or need to read attributes. This software is situated between the eID and the application, which is why it is sometimes referred to as 'middleware.' The installation of the software for the different combinations of equipment and versions of the operating system must be as simple as possible. The automatic distribution of the software without requiring user interaction is preferred.

Reliability

	Criteria	import	area	description
R01	10-year lifetime	M	G/M	The documents NIK and driving license have validity of 10 years. Because these documents may be carriers for the eID, a requirement is that the eID most support this lifetime. The card, chip, OS and application must be viable for 10 years.
R02	number of uses	M	G/M	The eID is used for public and private services, as well as for things like age verification when purchasing cigarettes or alcohol. This means that the eID must hold up to intensive use.
R03	contactless	S	G/M	A contactless eID has a longer lifetime than a contact chip. The estimate is that a contact chip will not last 10 years, which means extra costs for replacement. This requirement is also stipulated from a functional perspective, to allow mobile devices to be used as card readers in the future (NFC).

Performance

	Condition	Import	area	description
P01	transaction speed	M	G/M	The transaction speed for authentication must be shorter than 1 second after input of the PIN. This also applies for establishing 'proof' of age for retail transactions (alcohol, cigarettes).

Supportability

	Condition	Import	Area	description
S01	middleware	S	G/M	Support is important for eID. See U03. A problematic issue is the distribution of this middleware for different combinations of devices and operating system versions (Windows XP/Vista/7/8, Mac OS-X, Linux, IOS, Android). The automatic distribution of the software without requiring user interaction is preferred.

4.3.2 Requirements dictated by the market

For use by the market, the following additional requirements are stipulated. These requirements lie primarily in the privacy arena, because without them, acceptance and consequently use, will be low. See also the requirements formulated in the WBP.

Functionality

	Criteria	Import	Area	Description
F03	pseudonym (pseudo-ID)	S	M	The WBP requires that the design ensures sufficient protection of privacy. Using a pseudonym (pseudo-ID) when interacting with private parties prevents these parties from exchanging personal user data in order to compile a user profile.
F05	minimal disclosure	S	M	The WBP requires that the design ensures sufficient protection of privacy. Only the subset of the information required for the service may be provided. For certain transactions, for example, instead of providing the date of birth, a confirmation that the person is older than 18 will be sufficient.
F07	no hotspot	M	M	The Citizen Service Number (BSN) is required for government services to citizens, and may not be used outside of that domain. The eID system (the DigiD infrastructure) guarantees this. Special security measures are used to prevent undesired 'hotspots' from arising. For use in the market, required use of a central component (hotspot) is not acceptable from a privacy perspective because there is then one institution that can track which service providers individual citizens are authorising.
F08	unique identification	S	M	Private service providers must be able to uniquely identify users based on the municipal public records (personal data, i.e. name, address, etc.) where the user consents to the provision of this data.
F08	GBA attributes	S	M	Market parties often have a need for data registered by the government, such as age, address, etc. The assurance that a person is 18 or older, for example, may be used for access to a service without actually requiring establishment of the person's identity. Another example might be access to a waste dump that is restricted to local residents; only establishment of the city of residence is necessary. Consulting GBA attributes must be an option.
F09	other attributes	C	M	Attributes other than personal data may include membership in an association or entry in a register. For example, a patient may wish to establish whether a doctor has a BIG registration. In this case, only that registration need be provided.
F20	citizen-to-citizen	S	M	The eID must also be usable between citizens. For example, when entering into a contract over the internet, citizens must be able to identify themselves to an adequate degree so that in the event of failure to meet commitments, legal action can be taken without requiring further proof of identity (electronic signature, etc.).

Usability

No additional requirements dictated by the market.

Reliability

No additional requirements dictated by the market.

Performance

No additional requirements dictated by the market.

Supportability

No additional requirements dictated by the market.

5 Questionnaire

This chapter sets out the general questions about your organisation and the specific questions for this market consultation.

The questions are broken down into a number of subject areas:

1. Organisational details
2. General
3. Required conditions
4. Technology
5. Solution
6. eID system

Each subject area includes open questions. In addition to a yes or no answer, please provide an explanation of why you think so.
If you are only capable of supplying a portion of the eID solution, you only need answer the questions relating to your solution.
You may enter your answers on the answer sheet provided (in Word format).

5.1 Subject 1: Organisational details

5.1.1 Operating data

Question 1 Can you provide a description of your organisation and the products and services you supply?

Question 2 Could you please describe your motivation for participating in this market consultation?

Question 3 Starting at section 5.2, this RFI is broken down into a number of different subjects. Which of these subjects does your organisation have experience with and can you give a description of what that experience consists of?

Question 4 What recent (in the past three years) experience do you have in relation to the subject areas described in this market consultation?

5.2 Subject 2 General

5.2.1 Parcels and components

IKR envisions the following components which may be the object of tender:

1. a card with contactless chip and operating system;
2. personalisation of the card. A make-or-buy decision has yet to be made on this component;
3. middleware.

IKR envisions the following components as potentially coming from the market:

4. issue of authorisation certificates;
5. a server with service provider;
6. subsequent loading of certificates, such as electronic signatures.

Question 5 What opportunities and risks do you see in this distribution? Would you advise a different distribution, and if so, what and why?

Question 6 Which of the components 4-6 would your company tender for?

5.3 Subject 3 Key criteria

5.3.1 Key requirements

Question 7 The key requirements for an eID resource are listed in section 4.1. Can you indicate the opportunities and risks you see for each key requirement?

5.3.2 Privacy measures

Question 8 In addition to the key requirements, are there other requirements that might significantly contribute to protection of user privacy?

5.4 Subject 4 Technology

5.4.1 Contactless chip

Question 9 IKR intends to adhere to the following requirements for the DigiD card:

- the chip must have the capacity to be a reliable means of electronic authentication for a period of 10 years.
- the chip has a Common Criteria certification of at least EAL6+.
- the operating system has a Common Criteria certification of at least EAL6+.

Question 10 Do you have a product available that meets the above minimum requirements? If this product is not available for a 10-year period, do you have an equivalent alternative available?

Question 11 What is the minimal memory that is required for the eID application and the optionally loaded qualified certificate?

Question 12 How much time will your chip need for an RSA 2048-bit calculation, and how much for an ECC 256-bit calculation? (this in reference to chip performance)

5.4.2 Applications on the chip

Question 13 We envision a Common Criteria certification of the application at level EAL 4+. Is there a generally accepted protection profile and/ or security target as starting point for the common criteria certification? Please provide references.

Question 14 Can you deliver a Common Criteria certification of the application at level EAL 4+?

Question 15 Can multiple applications run on one chip without affecting each other or accessing each other's data? What are the required conditions to achieve this?

Question 16 Can additional applications subsequently be added to an existing card, or can existing applications on an existing card be changed, in a secure manner? If yes, does the additional application also have to be certified?

Question 17 Can a qualified certificate be added online to a card that is already issued, to allow use of a qualified electronic signature (QES)?

5.5 Subject 5 Solution

5.5.1 Own solution

Question 18 Does your company provide a solution that meets the key requirements given in section 4.1**Fout! Verwijzingsbron niet gevonden.**?

Question 19 Can you indicate on the table below which conditions your solution does and does not meet?

Requirements dictated by government:

Functionality

	Criteria	Import	Area	Compliant Yes/No	Explanation
F01	electronic ID	M	G		
F02	electronic signature	M	G/M		
F04	user consent	S	G/M		
F05	offline use	S	M/G		
F10a	mutual authentication	S	G/M		
F10b	purpose limitation	S	G/M		
F10c	Encryption or electronic signature	S	G/M		
F12	contactless communication	S	G/M		
F13	Loss/theft	M	G/M		
F14	high authentication level	M	G/M		
F15	proven technology	M	G/M		
F16	upgrading eID	S	G/M		
F17	European Citizen Card	S	G/M		
F18	European interoperability	M	G/M		

Usability

	Criteria	Import	area	Compliant Yes/No	Explanation
U01	metaphor	M	G/M		
U02	supporting OS	M	G/M		
U03	middleware	S	G/M		

Reliability

	Criteria	import	area	Compliant Yes/No	Explanation
R01	10-year lifetime	M	G/M		
R02	number of uses	M	G/M		
R03	contactless	S	G/M		

Performance

	Criteria	Import	area	Compliant Yes/No	Explanation
P01	transaction speed	M	G/M		

Supportability

	Criteria	Import	Area	Compliant Yes/No	Explanation
S01	middleware	S	G/M		

Requirements dictated by the market

Functionality

	Criteria	Import	Area	Compliant Yes/No	Explanation
F03	pseudonym (pseudo-ID)	S	M		
F05	minimal disclosure	S	M		
F07	no hotspot	M	M		
F08	unique identification	S	M		
F08	GBA attributes	S	M		
F09	other attributes	C	M		
F20	citizen-to-citizen	S	M		

Question 20 Is your solution regarded as proven and secure technology? For how many users is your solution used?

Question 21 Does the middleware required for the card to work with a device (NFC telephone or PC), need to be combined with the eID application, or can that be tendered separately? Can the middleware potentially also be developed as open source?

Question 22 Would a demonstration provide any added value to your responses to this questionnaire? What would you show in a demonstration to supplement this consultation?

5.5.2 Costs

Question 23 Can you give an indication of the cost of the card/chip/license for the eID application per user, based on the numbers in the table below?

In your answer, please specify separately the cost of:

- semi-manufactured card
- contactless chips with capacities ranging from 20 to 144 kB;
- the software license;
- personalizing semi-manufactured cards and contactless chip;

Question 24 In your responses, can you please make a distinction between (one time) investment costs and (yearly) operating costs for a contract duration of five years?

Year after introduction:	Number of cards
1st year	4 million
2nd year	3 million
3rd year	3 million
4th year	200,000
5th year	200,000

5.6 Subject 6 eID system

5.6.1 Implementation of the DigiD card

The DigiD card is intended to be a person-specific smartcard implementation of an authentication resource. In the role of authentication service, the government is the issuer of this authentication resource. The idea is for the citizen to be able to use this smartcard not only in the BSN domain, but also to log in with private service providers. In accordance with the design requirements, an authentication statement with a pseudo-ID is generated during the authentication process.
In the standard flowchart, the smartcard (in combination with the corresponding local smartcard middleware) makes contact with a central authentication service. This standard flow is presumably not difficult to support. However, this implementation scenario fails to utilize the full potential of a smartcard.

The goal is to allow the smartcard, working with local middleware running on the user's device, to supply an identification statement to the service provider even without the intervention of the central authentication service. This may be of importance in offline situations or if for considerations of privacy the user does not wish to leave any 'footprints' with a central authentication service (and other body of parties). This would create the potential for undesired privacy violation at the authentication service, being that the authentication service gathers knowledge concerning the user's login habits.

It would appear that with current, proven technologies it is very difficult to allow a smartcard (with corresponding local middleware) to generate an authentication statement in a reliable and anonymous manner in accordance with the requirements. Because in this case the authentication statement must be signed with a key on the smartcard, producing an authentication statement that is not traceable back to the individual seems to be problematic.

Question 25 Is it possible to sign an authentication statement with a certificate from an authentication service and under the responsibility of that service but without the intervention of the central authentication service?

Question 26 Are there alternatives by which the service provider can still derive adequate security from an authentication statement that is not signed or that is signed by the service provider itself?

Question 27 Are there any other conceivable solutions?