

Final report

UZI-register - supervised start-up

The CIBG completed its final report on a unique system of identification for Dutch healthcare providers (UZI-register) at the end of 2004. The aim of the UZI-register is to enable Dutch healthcare providers to be uniquely identified in electronic transactions. Along with the identification of Dutch healthcare consumers and Dutch healthcare insurers, the UZI-register is an important aspect of healthcare in the Netherlands. Since the unique identification of healthcare providers is also important beyond the borders of the Netherlands, and with a view to making the information more accessible, NICTIZ had this final report translated in January 2005.

In doing so, NICTIZ's intention is to provide other interested parties in and outside Europe with insight into the developments occurring in the Netherlands anno 2005. At the same time, the report can be a basis for opening discussions about standardization and interoperability between the various systems in use across Europe. You all are explicitly invited to discover how we are getting to grips with this issue in the Netherlands.

For further information about the UZI-register you are invited to visit the website: www.uzi-register.nl (even though the information given is mostly in Dutch at the time of writing, January 2005). We also recommend checking the NICTIZ website www.nictiz.nl to see if any further information has been translated into English.

Any queries or comments specifically relating to the UZI-register and the final report shall be submitted to the employees of the UZI register (info@uzi-register.nl). Any queries or comments about the Dutch healthcare infrastructure in general can be submitted to the undersigned.

N.B.: This English-language document is a translation. In the event of any ambiguity, the Dutch version should be consulted. No rights may be derived from this document.

Leidschendam, Netherlands - 19 January 2005

Johan G Beun, Ambassador of NICTIZ (beun@nictiz.nl).

Published by : Central Agency for Information on Healthcare Professions (CIBG)

Version : 1.0 Def. (Eng)

Date : 30-11-2004

© 2004 CIBG, Den Haag

All rights reserved. No part of this publication may be reproduced, stored in an automated datafile or made public in any form or in any way, whether electronically, mechanically, by photocopy, recording or any other means, without the prior written permission of the publisher: CIBG, telephone + 31 (0)70 340 7446.

Contents

Preface	4
1 Introduction	5
1.1 Introduction of UZI-register.....	5
1.2 Objectives of final report.....	5
1.3 Reading guide.....	6
2 Method used	7
2.1 Choice of method for supervised start-up.....	7
2.2 Evaluation.....	8
2.3 Consultation.....	8
2.4 Realization and certification.....	9
3 Consultation on recommendations	10
3.1 Session 1: Domain and number.....	10
3.2 Session 2: Policy and highest level trust point.....	11
3.3 Session 3: Certificate profile and infrastructure.....	11
3.4 Session 4: Card reader, card portfolio, demands of healthcare sector and points of issue..	13
4 National UZI-register	16
4.1 Objective and scope of UZI-register.....	16
4.2 Parties involved in the UZI-register.....	17
4.3 Types of UZI cards.....	19
4.4 Certificates.....	21
4.5 Life cycle of UZI card.....	22
Appendix 1: Abbreviations and concepts	26
Appendix 2: Related documentation	32
Appendix 3: Pilot projects	33
Appendix 4: Participants in consultation sessions	35
Appendix 5: Applicable standards	37

Preface

'Well, it's good to know that.' Dr. Bernard mutters quietly to himself as he removes his UZI card¹ from the card reader. He has just been checking the electronic patient record for details of a patient who came for an urgent consultation. Mrs. Ritsema, who lives in Friesland in the north of the country, is visiting her son and grandchildren in Utrecht. 'A contraindication for this medication, that is something I'll need to bear in mind.' Even a few years ago, the situation would have been quite different. He leans back, satisfied, tidies his hair and rushes off to meet the next patient.

This is not yet reality. But with the implementation of the UZI-register for the unique identification of healthcare providers in January 2005, one of the preconditions which will make this scenario possible will have been put in place.

A number of significant milestones have already been achieved on the road to implementing the UZI-register. For example: KPMG Certification carried out a certification audit and determined that the UZI-register which is being realized by the central agency for information on healthcare professions (CIBG) complies with the international ETSI TS 101456 standard, with Dutch legislation regulating electronic signatures and with the supplementary requirements laid down in the government's Public Key Infrastructure (PKI) for the Government domain and for Services certificates. Quite a list, but it means that CIBG is only the third organization, and the first government agency in the Netherlands which has been declared competent to issue legally valid electronic signatures.

Another important milestone is this final report: the final report on the project 'UZI-register - supervised start-up, in which you can learn how the UZI-register will be organized and how the choices in that respect came about. During the project it proved useful to have sound foundations in the form of principles and explanations. These provided a hand-hold in the struggle through the turbulence in which all those of us who have been involved in creating such an innovative service as the electronic patient record find ourselves. I hope and expect that this final report will also be useful to others.

Without contributions from various other parties it would never have been possible to achieve this milestone. And for that reason I would like to offer a vote of thanks to everyone who helped with the organization of the UZI-register. I am thinking, for example, of the people who took part in the pilot projects, in the interviews, and the participants in informative and consultative sessions, and also the colleagues from the Ministries of Public Health, Welfare & Sports and the Interior & Kingdom Relations. A sincere thank you to you all!

J.G.P. Huisman
Director, Central Agency for Information on Healthcare Professions

¹ A glossary of abbreviations, acronyms and concepts has been included in Appendix 1.

1 Introduction

1.1 Introduction of UZI-register

If it is to be possible to conduct secure electronic communications and referencing of confidential information in the healthcare sector, it will be essential to have a unique identification system for all parties concerned. For that purpose, the Unique Healthcare Provider Identification Register (UZI-register²) has been set up to facilitate the unique identification and authentication of care providers³. The identification system for the healthcare sector recognizes the importance of identification, not only for healthcare providers but also for the consumers and users of care services and for healthcare insurers.

When a healthcare practitioner tries to access the information system of a hospital, for instance, the identity of that practitioner must be known. Quite often it is not only necessary to determine the applicant's identity but also to ascertain, with certainty, that it is the healthcare practitioner himself and not some other person. Similarly, the healthcare practitioner will want to be sure that the information system is actually associated with the hospital. Both parties must be able to identify themselves unequivocally in electronic communications.

When information - a diagnosis, for example - is being exchanged between the healthcare practitioner and the information system, certainty must be provided that only the healthcare practitioner himself, and no other person, can read that diagnosis. This clearly makes demands on the confidentiality of the communication.

There is an increasing need in the domain of electronic communications for an electronic signature by which it would be possible, for example, to determine irrefutably that the healthcare practitioner has made a particular diagnosis.

The UZI-register offers a solution in situations such as this.

For this purpose the UZI-register will issue healthcare providers with an electronic identity, in the form of a UZI card, by which they can identify and authenticate themselves, by which they can guarantee the confidentiality of the communication and by which they can enter an electronic signature.

1.2 Objectives of final report

The object of the UZI-register supervised start-up project is to test the choices made from the definition study⁴ with regard to the organization, the trust framework and the architecture of the UZI-register in practice, and to refine those choices where necessary. The UZI-register will then be organized on the basis of the results of the pilot project.

The aim of the final report you now have before you is to provide insight into the choices which have been made on the basis of the tests carried out during the supervised start-up. To this end, the final report contains an overview of these choices and a brief explanation. For further details please refer to the advisory reports.

² UZI-register is a registered name.

³ The concept 'healthcare professional' is here taken to include all healthcare practitioners and the representatives, employees and systems of healthcare institutions. A glossary of terms has been included in Appendix 1.

⁴ For an overview of the documentation from the preliminary studies which preceded the supervised start of this project, and for the definition study, the reader is referred to Appendix 2.

1.3 Reading guide

Chapter 2 explains the method used for the UZI-register supervised start-up project. Chapter 3 then provides a description of the recommendations of the consultative sessions. Finally, chapter 4 describes the UZI-register as it will be realized on the basis of the resulting recommendations.

2 Method used

CIBG carried out the supervised start-up project on the UZI-register at the commission of the Ministry of Health, Welfare & Sports. The object of the project is to test the choices made from the advance definition study with regard to the organization, the confidential framework and the architecture of the UZI-register in practice, and to refine those choices where necessary. In this chapter we shall describe the method used to assess the project.

2.1 Choice of method for supervised start-up

During the definition study, a design was made for the UZI-register and investigations were carried out to ascertain how this design could be implemented in technical terms. On the basis of the results of the definition study, it could be concluded that it would be essential to start using the UZI-register in a limited number of controlled environments (pilot projects). This was necessary in order to be able to test and where necessary modify the organization, the trust model and the technical infrastructure. At the same time, the supervised start-up provided other parties with the opportunity to investigate associated issues (such as authorization) and to put the administrative and legal preconditions in place. As far as the UZI-register is concerned, this method offered the opportunity to introduce the scheme in a controlled and phased manner, while testing and improving service on the way.

In order to implement the necessary checks, the size of the UZI-register was restricted during the supervised start-up. The experiences gained during the UZI-register supervised start-up phase were then evaluated. The findings of the evaluation were used to define the specifications for the national UZI-register, and formed the basis for recommendations to the Minister for Health, Welfare & Sports on a number of important issues. Before these recommendations were submitted to the Minister, experts and interested parties were informed about and consulted on the recommendations. Figure 1 illustrates the method used.

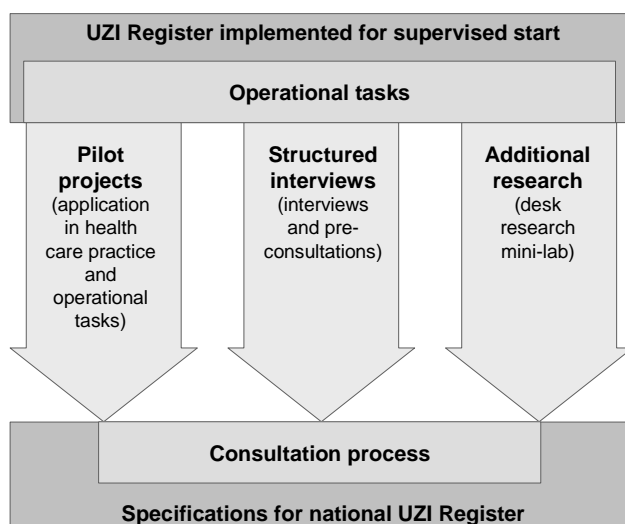


Figure 1: testing and evaluation method

2.2 Evaluation

During the supervised start-up, evaluation was carried out on the basis of the three categories illustrated in Figure 1, i.e. pilot projects, structured interviews and further research.

The first category comprised the pilot projects. Appendix 3 gives a summary of the pilot projects involved. During these pilots, UZI cards were used in various practical situations and healthcare applications. Different groups of healthcare practitioners were involved: GPs, pharmacists, a dentist, a physiotherapist along with a number of medical specialists. A total of 120 cards were issued, 50 of which were test cards for ICT support staff and application developers. Although the UZI card could be used successfully in many cases, the pilot projects did highlight the fact that its use is accompanied by a number of operational challenges. The experience gained in the pilot projects were incorporated into the resulting recommendations. One thing that was changed as a result of the pilot projects was the UZI-register's card portfolio.

The second evaluation category consisted of structured interviews and pre-consultation. During the structured interviews, practical experiences and opinions were collected about the healthcare processes within which the UZI card could best be used, the basic requirements for the issuing process and the decision about whether or not to incorporate a photograph into the card. The pre-consultation consisted of interviews with people which specific expertise in a particular area, during which proposed recommendations could be further refined and checked. Pre-consultations were held with various parties on subjects such as certificate profiles.

The third and final category concerns further research. Desk research was carried out into developments on the international front which are comparable to the UZI-register. National experiences, such as those gained by the Zorgpasgroep, a collaborative forum representing patients, doctors, hospitals, paramedic professions and health insurers, were also taken into account. Laboratory tests were also carried out. These mainly involved verifying the present status of technical possibilities and impossibilities, and looking into the options for UZI services certificates.

2.3 Consultation

Four consultation sessions were organized by the UZI-register in the period between March and September 2004. The aim of these sessions was to facilitate an appraisal of the choices made in various domains on the basis of the evaluation against the experience and expertise gained in practice.

The sessions were announced on the website and a wide range of interested parties and experts were invited to attend. In the event of specific opposition to any recommendation presented, those attending were asked to explain their opposition using an actual practical case as an example.

Immediately after the consultation session, the consultation memo was published on the UZI-register's public website; practitioners in the field were then invited to report any contraindications.

After each round of consultations, the consultation memo and the contraindications submitted formed the basis for a memo of recommendations which was sent to the Minister for Health, Welfare & Sports. A summary of these recommendations can be found in Chapter 3 of this final report.

The consultation sessions were well attended by a wide variety of experts. Responses were also received via the website. A list of participants in the consultation sessions and the people who responded via the website can be found in Appendix 4.

2.4 Realization and certification

During 2004 a start was also made with the realization of the national UZI-register. Preparations for the tendering process were made at the same time as the consultations on the recommendations. From September 2004 work has been in progress on the practical realization of the scheme on the basis of the final recommendations. It is expected that the first UZI cards for the definite national UZI-register can be issued in January 2005.

KPMG Certification carried out an audit at the beginning of November 2004. The audit confirmed that the UZI-register complies with the international ETSI TS 101456 standard⁵, with Dutch legislation regulating electronic signatures and with the supplementary requirements laid down in the government's Public Key Infrastructure (PKI) for the Government domain and for Services certificates. This means that the UZI-register can now apply for registration to the Dutch OPTA (Independent Post & Telecommunications Authority) and can join the government PKI hierarchy.

⁵ A summary of the standards which are used by the UZI-register has been included as Appendix 5.

3 Consultation on recommendations

Four consultation sessions were held in the course of 2004 on the basis of the concept described previously. This chapter provides a summary of the recommendations which were formulated at the consultation sessions, and of the reactions which followed their publication. The recommendations have been grouped per session. For a detailed rationale of the recommendations and the options considered, please see the individual session memos.

3.1 Session 1: Domain and number

The first consultation session, on the theme 'UZI domain and number', took place on 30 March 2004. The central issues for this session were the demarcation of the domain (who can obtain a UZI card, and for what purposes may it be used), and the choice for the number that needs to be included in the certificate to ensure that the certificate holder is uniquely recognizable.

Recommendation 1: *Only those healthcare providers who need to have access to the health data of persons for the purposes of their work may be included in the UZI-register.*

The domain of the UZI-register is related to the necessity to have active access to the health data of persons. This restriction of the extent of the domain to care providers who potentially need access to such health data, will make it possible to allow direct access to this data in emergency situations. It will, of course, be necessary in such emergency situations to have an appropriate system for logging such access so that retrospective accountability can be assured.

Recommendation 2: *The UZI domain is not a closed domain.*

This recommendation centres on use of the UZI card not being subject to the condition that all communicating parties need to belong to the UZI domain. The use of the UZI card within the healthcare domain is, however, both desirable and possible.

Recommendation 3: *The UZI number is a new number in the healthcare sector which can be used for authentication and to ensure non-repudiation in electronic communications.*

In both the preliminary stages and during the consultations it was considered using an existing numbering scheme such as the AGB code (as used for healthcare practitioners and care institutions; see App. 1) for the UZI card. But this proved to be unfeasible for a number of reasons. The ultimate recommendation means the introduction of a new number in the healthcare sector. The UZI number can be used for authentication and to ensure non-repudiation in electronic communications, alongside the existing numbers used in administrative and expense claim processes. The Minister for Health, Welfare & Sports has also been advised to investigate whether a single unique identifying number for healthcare might be desirable and feasible in the longer term.

Recommendation 4: *A personalized UZI number is issued to healthcare practitioners and the staff of a healthcare institution who are authenticated by the UZI-register. The UZI-register issues a non-personalized institution-linked number for the 'services' of care institutions and for the staff of care institutions who are authenticated at an institutional level.*

The desire of those working in the healthcare sector to be able to identify healthcare providers irrespective of time and place makes it necessary to have a personalized UZI number which makes it possible to identify individual healthcare practitioners and members of staff. A direct consequence of a personalized number is the need for the UZI card to be issued to the holder personally. By definition, services (i.e. systems, websites, databases and so on) will also be given a new number. The

authentication of staff of healthcare institutions who work within those institutions will be regulated by the institution itself. In such cases, the obvious choice would be an institution-linked UZI number.

3.2 Session 2: Policy and highest level trust point

The second consultation session, held on 11 May 2004, concentrated on organizational and policy issues.

Recommendation 1: *The implementation of the UZI-register is a public task which should be carried out by an organization governed by public law.*

Because of the public interest and the vested interests involved, the introduction of the UZI-register is a public task with a clear role for the Minister for Public Health, Welfare & Sports. In view of the Minister's responsibility, the administration of the UZI-register should be in the hands of a body governed by public law. It is only through administration of the register by a public law organization that the Minister will have sufficient opportunity to substantiate this responsibility.

As a footnote to this recommendation, it can now be reported that the Minister for Public Health, Welfare & Sports has meanwhile commissioned the CIBG to administer the UZI-register.

Recommendation 2: *The UZI-register designates the root certificate of the State of the Netherlands as its highest level trust point, and wishes to be incorporated into the hierarchy of the government PKI as a Certification Service Provider (CSP). In doing so, the UZI-register chooses to comply with the requirements of the government PKI.*

The healthcare sector's desire for reliable and secure electronic communication and access to electronically stored data is by no means unique. The schedule of requirements for the government PKI provides for a framework of standards for the services of the UZI-register, a pre-defined level of security that is transparent for card holders and relying parties, and independent monitoring and supervision. Fulfilling the requirements of the government PKI, and being incorporated into the hierarchy of the government PKI means that optimum use can be made of existing frameworks and past experience. The choice of the State of the Netherlands as the highest level trust point for the UZI cards gives a clear signal to relying parties; this will also apply in possible international dealings.

Recommendation 3: *The Minister for Health, Welfare & Sports determines the healthcare-specific policy for the UZI-register. This policy includes the actual demarcation of the UZI domain. The Minister for Health, Welfare & Sports will be advised by the healthcare sector on this point.*

The Minister for Public Health, Welfare & Sports is the most appropriate person to determine policies with regard to healthcare-specific aspects of the UZI-register. In doing so, the Minister will take advice from the sector.

In the context of that advice it can be noted that the UZI-register is proposing to advise the Minister for Public Health, Welfare & Sports by means of consultation sessions.

3.3 Session 3: Certificate profile and infrastructure

The theme of the third session, held on 22 June 2004, was the certificate profile and the infrastructure. These subjects are at the core of the UZI-register. The certificate profile is set up in such a way as to answer questions such as: 'Who is the card holder?' and 'What is the card holder?'. The first of these questions relates to the actual person holding the card, the second to the status of the care provider

represented by the card holder. The questions 'What may the card holder do?' or 'What data has the card holder viewed or modified?' cannot be answered by the UZI-register.

Recommendation 1: *The UZI-register makes use of the three certificate model, with separate certificates for the functions of authentication, confidentiality and non-repudiation (electronic signature).*

The healthcare sector has expressed a clear need for an electronic signature, especially for inter-institutional electronic communications, for instance in expense claim messages and prescriptions, where a doctor will want to append his signature to a prescription for a pharmacist or to a diagnosis he has made. In addition, the electronic signature is important when it comes to signing contracts with healthcare insurers, for instance, or with colleagues in the context of locum services. The legal force of the electronic signature must be equal to that of a written signature. In view of this objective and with a view to optimum assurance of reliability and security, the UZI-register opts for a separate certificate for the authentication, confidentiality and - via an electronic signature - non-repudiation functions. Although not all standard applications correspond well with the three certificate model, it was found during the supervised start-up that the three certificate model can nonetheless be applied correctly with the help of relatively simple aids. A final comment is that this choice complies with the schedule of requirements drawn up for the government PKI.

Recommendation 2: *The UZI-register's certificate profiles are drawn up in accordance with the schedule of requirements for the government PKI. The link between the UZI certificates and the review registers will not be incorporated in the UZI certificate. The certificate profile leaves space for the inclusion of a single AGB number (AGB: see App. 1). The AGB number will be included in the certificate if its accuracy can be guaranteed by the UZI-register. The UZI-register's certificate profiles include space for a standardized role description. This role will be entered on the basis of the professional titles defined in the Individual Healthcare Professions Act [Wet Beroepen in de individuele Gezondheidszorg Wet, BIG] The legally protected title will be used for medical specialists. If the Minister designates new professional groups, the professional and possible specialist titles to be used for these groups will be defined.*

The UZI-register's certificate profiles are drawn up in accordance with the schedule of requirements for the government PKI (Part 3, version 5). This is in accordance with the advice to incorporate the UZI-register into the government PKI and to operate the Register under the root certificate of the State of the Netherlands. Healthcare-specific requirements will be fulfilled within the framework of the overall schedule of requirements.

A link between a UZI certificate and the review register is desirable because it will provide a relying party with any additional information about the healthcare provider it might require. This link will be effected outside the UZI certificate.

A number of stakeholders have requested the inclusion of an AGB number. Its inclusion will mean that the UZI certificates will be more widely applicable within the healthcare domain. The AGB number can only be included in the certificate if its accuracy can be guaranteed by the UZI-register. The certificate provides space for a single AGB number.

The UZI certificate must contain sufficient details so that authorization is possible. The certificate profiles allow space for the inclusion of both a professional title and a possible specialism. These details are encoded for automated processing, but are also legible in the form of a courtesy title for human use.

Recommendation 3: *The UZI-register institutes a PKI on the basis of a Certification Authority model (CA model) with five CAs: one UZI CA with four sub-CAs for healthcare practitioners, for named employees, for employees in general and for services. The UZI-register will institute a key escrow service for the issuing of confidentiality keys.*

The Certification Authority (CA) is the entity which is trusted by the end users to create and issue certificates: it is in fact the technical heart of the UZI-register where the keys of all card holders are certified. The UZI-register has elected to follow a CA model, with one CA and four sub-CAs. From the point of view of communications it would be advisable to have the various types of cards countersigned by different sub-CAs so that - once in use - they can easily be distinguished on the basis of the issuing CA or sub-CA. If relying parties do not wish to accept certain types of certificates, it will then be simple to achieve this exclusion on the basis of the issuing (sub) CA.

Data can be encrypted with the aid of the confidentiality key on the UZI card and hence rendered illegible for others for the purposes of transmission or storage. It is only with the aid of the private confidentiality key that this data can again be made legible. This means that if the UZI card is lost or stolen, it will not be possible - in principle - to render that data legible again. In order to circumvent problems of this nature, all subscribers and card holders must take appropriate measures. Specific circumstances can, however, arise in which these measures prove to be inadequate or impractical. For that reason, and to safeguard the interests of healthcare, the UZI-register will provide a compulsory key escrow service (backup of private confidentiality keys) to all subscribers.

Recommendation 4: *The UZI-register elects to use the smart card as the carrier of keys and certificates for healthcare practitioners and for the employees of healthcare institutions. The UZI-register elects to use a six digit PIN code as the activation code for those smart cards. For the future, the UZI-register is bearing in mind the incorporation of other carriers which comply with the requirements of the government PKI, and with other types of activation.*

The UZI-register elects to use the smart card as the healthcare-sector-wide carrier of its keys and certificates. At the moment there are no other carriers available which comply with the security requirements as defined. In the longer term it is possible that other carriers will become eligible.

The UZI-register elects to use a PIN code as the activation code for the UZI card. During the supervised start-up, a number of queries were raised from the healthcare sector about the application of other activation techniques, including the use of biometrics. Potentially, the application of biometrics would not only increase security but would also ensure personal use. However, the stage of development of the technology⁶ concerned and the higher costs make the use of biometrics undesirable in the short term. The UZI-register will be following developments in the field of activation closely.

3.4 Session 4: Card reader, card portfolio, demands of healthcare sector and points of issue

The fourth and final consultation session took place on 30 September 2004. The 'PKI middleware and card readers' issue was mainly concerned with technical aspects, while the other three issues were more closely related to practical aspects concerning healthcare providers and processes. 'Which cards will be necessary to support healthcare processes to an optimum degree' and 'How can those cards be delivered to the care provider in the most effective way' were the most important questions to be answered.

⁶ At the moment, biometric technology is still flawed, resulting in both unjustified recognition and unjustified rejection.

Recommendation 1: *On its institution, the UZI-register will guarantee the working of the UZI card in combination with a limited range of card readers and PKI middleware. This initial set of combinations guaranteed by the UZI-register will be extended as and when appropriate in connection with applicability in the practical healthcare domain. Initially the UZI-register elects to use card readers without their own operating system but based on relevant standards and interfaces. The UZI-register supports the working of the UZI card in environments with designated versions of the MS Windows, Linux and Mac operating systems. The UZI-register will follow relevant developments in this area, and it is to be expected that the present restrictions will disappear in the course of time.*

In order to be able to make use of the keys stored on the card in practical healthcare situations, the important issues are details of the PC, the card reader and the card itself. Up to now there has been no integrated implementation of open standards with regard to these components. With a view to optimum assurance of reliability and security, the UZI-register prefers to guarantee the working of the UZI card with only a limited set of combinations of card readers and middleware. This leads the UZI-register to necessarily make an initial choice for a solution which is dependent on one or a small number of suppliers. Initially, the UZI-register chooses card readers which have no inbuilt operating system. The use of other types of card readers is not totally excluded however.

In making the necessary choices, the UZI-register will endeavour as far as possible to link up with the operating systems generally used in the healthcare sector.

Recommendation 2: *The UZI-register's portfolio consists of the following cards:*

- *Healthcare provider, for people in respect of whom the UZI-register can guarantee not only the personal identity but also the 'status of healthcare practitioner' and the relationship to the subscriber.*
- *Named healthcare employee, for people in respect of whom the UZI-register can guarantee not only the personal identity but also the relationship to the subscriber.*
- *General (non-specific) healthcare employee, for people in respect of whom the UZI-register can guarantee the relationship to the subscriber.*
- *Services, for systems or websites, for example, in respect of which the UZI-register can guarantee the relationship to the subscriber.*

The aim of the UZI card is to uniquely identify and authenticate healthcare providers. The questions: 'Who is the card holder?' and 'What is the card holder?' are the most important issues. The first question relates to the actual person who holds the card. The UZI card offers certainty about the identity of the card holder. The second question relates to the status of the card holder as a healthcare provider. The UZI card provides a clear answer to the question of whether the card holder is a healthcare practitioner and whether he is working on behalf of a healthcare institution. In the light of these questions, the UZI-register elects to use an appropriate model for cards which addresses these concerns.

Recommendation 3: *In organizing the issuing process, the UZI-register will be guided wherever possible by the following requirements formulated by the field:*

- *Guaranteed high-level of reliability, assured by uniform procedures and controls.*
 - *A maximum of 5 working days between the approved application and actual issue, with the issuing process taking a maximum of 5 minutes.*
 - *Issue to be effected at a well-secured location within 20 minutes travelling time of the healthcare provider's location.*
 - *The healthcare practitioner or named employee will need to appear in person only once.*
-

- *Transparent issuing process involving the appending of just one signature, with good advance information.*

Users of UZI cards and relying parties from the healthcare domain alike make demands on the issuing process of the UZI card. The demands relate to the reliability and timeliness of the issuing process, and to the locations where cards will actually be issued. The UZI-register will take the demands of the field in respect of the issuing process of UZI cards as its benchmark for the final organization of the register.

Recommendation 4: *With regard to the location of the various processes of the UZI-register, it has been decided to have a central location where registration, control and production processes will take place; the UZI-register will endeavour to deal with as much as the registration process as possible via the internet. The issuing of UZI cards will take place at decentral locations in an environment which:*

- *is easily accessible for the healthcare provider;*
- *can guarantee a high security level;*
- *has both the quality and the capacity to provide the service;*
- *can offer a good price/quality ratio.*

It is recommended that post offices should initially be used as the point of issue. In future, other and additional locations are possible.

Some of the tasks of the UZI-register can be carried out either centrally or decentrally. The UZI-register opts to have the registration, control and production processes of the register carried out at a central location. The registration process will be effected as far as possible via the internet, so that registration in the UZI-register and an application for a UZI card will involve the minimum of effort. A specialized service provider (PinkRocade) has been contracted for the production processes. The UZI-register opts to carry out the issuing process decentrally, as close as possible to the healthcare provider's physical location. In view of the strict requirements of the issuing process, the UZI-register opts initially for a single partner to carry out the process. For the issuing of the UZI card, a contract has been concluded with a specialist service provider in the form of Netherlands Post Offices B.V. (B.V. = Ltd.).

4 National UZI-register

The UZI-register will be organized on the basis of experience gained in the supervised start-up and the recommendations approved by the Minister for Public Health, Welfare & Sports. This present chapter sets out the main lines of the various aspects of the UZI-register.

4.1 Objective and scope of UZI-register

The objective of the UZI-register is to identify healthcare providers uniquely for the purpose of electronic communication and access to data. For this purpose, the UZI-register creates a unique link between the physical identity of the care provider and an electronic identity, which is then recorded in certificates. The certificates and the associated cryptographic keys are stored on a smart card; the entirety of smart card, keys and certificates is referred to as a UZI card⁷.

In the identification and authentication of healthcare providers, the primary questions are: 'Who is the card holder?' and 'What is the card holder?'. The first question relates to the actual person who holds the card. The UZI card offers certainty about the identity of the card holder. The second question relates to the status of the card holder as a healthcare provider. The UZI card provides certainty about whether the card holder is a healthcare practitioner or an employee, and whether the card holder is working on behalf of a healthcare institution or a healthcare practitioner.

The holder of a UZI card can use the card to authenticate himself when seeking access to data. Examples are: seeking access to a secure website or to the referral index for the electronic medication record. In addition, the UZI card can be used to protect data against undesired access or alteration. An example of this is secured email via the internet. Finally, the UZI card can also be used to place an electronic signature.

Before an explanation is given of the various aspects of the UZI-register, it is necessary to briefly consider the concept of healthcare provider. In this context, healthcare providers are those categories of healthcare practitioners and institutions which are so designated by the Minister for Public Health, Welfare & Sports.

- | | |
|-------------------------|--|
| Healthcare practitioner | <ol style="list-style-type: none">a. An independent healthcare practitioner as intended in Articles 3 and 34 of the Individual Healthcare Professions Act [<i>Wet Beroepen in de individuele Gezondheidszorg Wet (BIG)</i>] and further referred to as the BIG Act].b. A joint venture between professional practitioners as intended in Articles 3 and 34 of the BIG Act, for the purpose of which facilities may be shared but there is no joint responsibility for care or any hierarchy between practitioners.c. Solo operating healthcare practitioner, as intended in Articles 3 and 34 of the BIG Act, who works with one or more auxiliary persons (in a hierarchical arrangement for the purpose of providing healthcare services). |
| Healthcare institution | <ol style="list-style-type: none">a. An organizational entity as intended in the Quality of Healthcare Institutions Act [<i>Kwaliteitswet zorginstellingen, KwZ</i>].b. A joint venture between practitioners as intended in Articles 3 and 34 of the BIG Act, whereby there is joint responsibility for care and care by multiple practitioners is coordinated. |

In the context of these categories, it is important to note that the KwZ does not recognize the concept of a joint venture between practitioners in a so-called 'healthcare practice'. Depending on the nature of

⁷ The concept 'UZI card' is used to describe the certificates, keys and the associated holder. The term 'UZI card' is used even when the information carrier is other than a smart card.

the collaboration within a 'healthcare practice', this can be deemed to be a healthcare practitioner or a healthcare institution.

4.2 Parties involved in the UZI-register

A number of different parties are important if the identification and authentication of healthcare providers is to be effected in a reliable and controlled manner. The most important parties are the care providers and the relying parties; these are the end users of the products of the UZI-register. In addition, a certification service provider is necessary, a party who arranges the registration of healthcare providers, the production and issuing of the UZI card and the publication of the necessary information. This certification service provider must work in accordance with certain standards and guidelines. Finally, there are parties who supervise these standards and guidelines and compliance with them. The parties involved are represented schematically in the following figure.

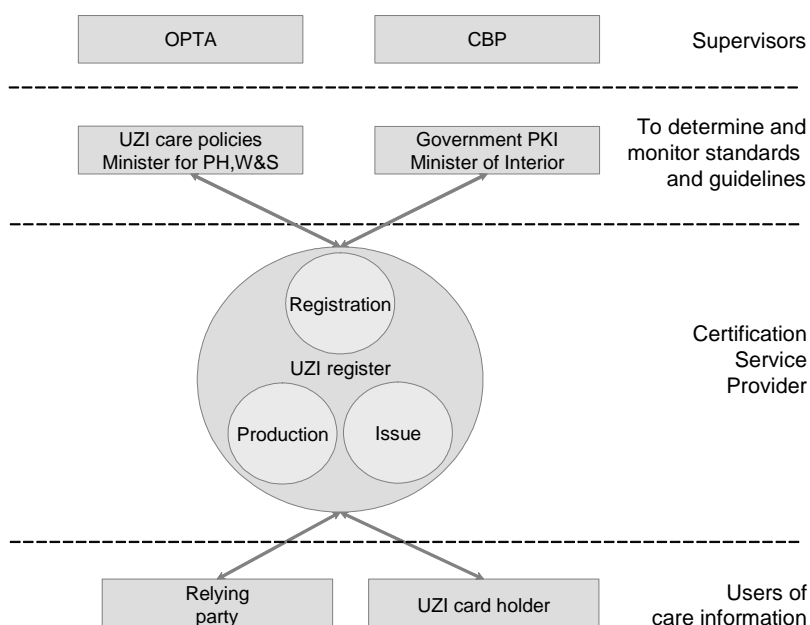


Figure 1: Parties involved

4.2.1 Users of healthcare information

In order to make use of UZI cards, a healthcare provider must become a subscriber to the UZI-register. A subscriber is a natural person or an incorporated entity who/which concludes an agreement with the UZI-register by which this person/entity becomes a user of certification services. Healthcare institutions and healthcare practitioners⁸ who are not employed by an institution (hereafter to be referred to as an 'individual healthcare practitioner') can register as subscribers to the UZI-register.

An additional requirement for practitioners as intended in Article 3 of the BIG Act is that they have enrolled in the BIG Register and have not been unconditionally suspended. In the first instance, the enrolment of practitioners, as intended in Article 34, is restricted to healthcare providers who have enrolled in the Quality Register for Paramedics⁹ [*Kwaliteitsregister Paramedic*]. Only a subscriber can

⁸ As described in section 4.1.

⁹ During 2005, the UZI-register will be investigating whether any other registration system (governed by public law) can be used for the screening of practitioners as referred to in Article 34 of the Individual Healthcare Professions Act [*Wet Beroepen in de individuele Gezondheidszorg Wet, BIG Act*].

apply for UZI cards. If a subscriber is a natural person requesting a card for him or herself, that subscriber then also becomes the UZI card holder.

A UZI card holder is a natural person who is characterized in the certificate as the holder of a private key that is linked to the public key specified in the certificate. The card holder is related to the subscriber specified in the certificate.

A relying party is the natural person or legal entity who/which is the recipient of a certificate (a message signed with the aid of a UZI card, for instance) and who acts in reliance on that certificate. The category of relying parties consists of everyone who acts in reliance on certificates from the UZI-register; possible aims are authentication of care providers, verification of an electronic signature or the encryption of communications with the party concerned.

4.2.2 Certificate Service Provider

The UZI-register unit to be established at the CIBG will fulfil the role of certification service provider and have final responsibility for the delivery of certification services. The UZI-register itself will take care of the processing of applications for certificates and all associated tasks. The UZI-register will physically collate identification data, check and register this data, and carry out the prescribed checks and verification. Once all these checks have been carried out, the Certification Authority (CA) will be instructed to produce the UZI cards and publish the relevant certificates.

The CA produces and publishes certificates and certificate revocation lists (CRLs). It does so on the basis of an authenticated request from a registration clerk attached to the UZI-register. Certificates are published immediately after they have been created by the CA. If certificates need to be invalidated before the expiry date shown in the certificate, the CA will publish the number of the certificates on the Certificate Revocation Lists (CRLs).

The CIBG has contracted distribution and issuance of the UZI cards out to Netherlands Post Offices. After verifying the identity of the intended card holder, this organization will physically hand over the UZI card.

4.2.3 Determining and monitoring standards and guidelines

The standards and guidelines with which the UZI-register must comply are determined by two separate ministries, i.e. the Ministry of Public Health, Welfare & Sports and the Policy Authority of the government PKI as a representative of the Ministry of the Interior and Kingdom Relations (BZK).

The Minister for Public Health, Welfare & Sports determines which persons and organizations belong to the domain covered by the UZI-register and with the aid of which procedures checks must be carried out to determine that these persons and organizations actually belong to that domain. Moreover, the Minister must ensure that the UZI-register, as a Certification Service Provider, supplies products which are the most appropriate for the healthcare sector.

As the UZI-register has elected to nominate the State of the Netherlands as the highest level trust point for the root certificate, the standards and guidelines determined by the Policy Authority for the government PKI must be complied with.

4.2.4 Supervisors

Both the Minister for Public Health, Welfare & Sports and the Policy Authority for the government PKI act as supervisors for the UZI-register. The OPTA and the Dutch Data Protection Authority [*College bescherming persoonsgegevens*] also play an important supervisory role.

OPTA is the watchdog organization for the postal and telecoms market in the Netherlands. The tasks and powers of OPTA are set down in laws. The Electronic Signatures Act [*Wet elektronische*

handtekeningen] stipulates that a certification service provider which issues qualified certificates to the public must be registered with OPTA. The fact that the UZI-register has officially been registered with OPTA is an indication that all statutory requirements have been fulfilled. Registration with OPTA does not, however, signify that OPTA warrants, or can be held responsible for, the actual quality of the UZI-register. After registration, OPTA will verify that the UZI-register continues to comply with all the requirements of the law. OPTA is empowered to terminate registration if the UZI-register fails in this respect.

As indicated above, the UZI-register will record various personal details. In doing so, the UZI-register will have to comply with the provisions of the Personal Data Protection Act [*Wet Bescherming Persoonsgegevens*, WBP]. If no exemption has been granted, the processing of personal details must always be notified in advance to the Data Protection Authority. The Authority maintains a public register of such notifications. The lawful basis of certain processing tasks, which are accompanied by exceptional risks, also needs to be ascertained by the Authority in advance. The Data Protection Authority (previously known as the Dutch Privacy and Data Protection Authority) was instituted to supervise compliance with the Personal Data Protection Act and other statutory provisions relating to the protection of personal details. The UZI-register has fulfilled its obligation to notify the Data Protection Authority.

4.3 Types of UZI cards

The UZI-register will issue UZI cards which can be used by healthcare providers. These are categories of healthcare professionals and practitioners and healthcare institutions which have been thus designated by the Minister for Health, Welfare & Sports, as already explained above. The various card types are illustrated in the following figure.

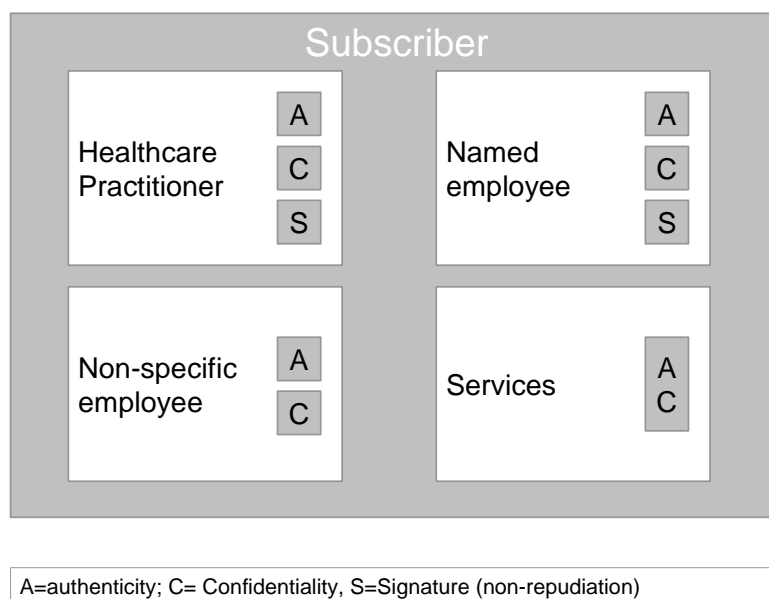


Figure 2: Card portfolio and certificates

4.3.1 Healthcare practitioner

The Healthcare Practitioner UZI card is for professional practitioners as intended in Articles 3 and 34 of the Individual Healthcare Professions Act [*Wet Beroepen in de individuele Gezondheidszorg Wet, BIG Act*]. Issue of the card is effected on the basis of a face-to-face check and verification of the legal identity, after a check has been made in the BIG Register or the Quality Register for Paramedics

[*Kwaliteitsregister paramedic*] that the person in question is eligible for the status of healthcare practitioner. Besides the identity of the individual, the UZI-register also guarantees the 'status of healthcare practitioner' and the relationship to the subscriber. Healthcare practitioners receive a personalized card which includes a photograph, and three certificates and key pairs (authentication, confidentiality and non-repudiation).

There are two types of cards for healthcare providers.

- individual practitioner: if the subscriber is an independent healthcare practitioner
- institution-linked practitioner: if the subscriber is a healthcare institution in the sense of the Quality of Healthcare Institutions Act [*Kwaliteitswet zorginstellingen*].

4.3.2 *Named employee*

An employee of an organizational entity as intended in the Quality of Healthcare Institutions Act, or a person who is designated by an individual practitioner as an auxiliary¹⁰, can be issued with a card of the type 'Named employee'. The card must always be requested by a subscriber. Issue of the card is effected on the basis of a face-to-face check and verification of the legal identity. Besides the identity of the individual, the UZI-register also guarantees the relationship to the subscriber. Named employees receive a personalized card which includes a photograph, and three certificates and key pairs (authentication, confidentiality and non-repudiation).

For the time being, cards for named employees will only be issued to subscribers which are healthcare institutions as intended in the Quality of Healthcare Institutions Act. The issue of cards for subscribers who are individual practitioners is expected to commence in the near future.

4.3.3 *Non-specific employee*

An employee of an organizational entity as intended in the Quality of Healthcare Institutions Act, or a person who is designated by an individual practitioner as an auxiliary, can be issued with a card of the type 'Non-specific employee'. The certificates on this UZI card indicate that the card holder is an employee of the subscriber who is named in the certificates. The subscriber is responsible for the accuracy of the details on the employee's certificates. The UZI-register guarantees the relationship to the subscriber. Employees with the non-specific employee status receive a non-personalized UZI card with two certificates and key pairs (authentication and confidentiality).

For the time being, cards for non-specific employees will only be issued to subscribers which are healthcare institutions as intended in the Quality of Healthcare Institutions Act. The issue of these cards for subscribers who are individual practitioners is expected to commence in the near future.

4.3.4 *Services*

Services (e.g. applications, websites, servers, etc.) of an organizational entity as intended in the Quality of Healthcare Institutions Act or of an individual healthcare practitioner can be issued with a card of the type 'Services'. The certificates on this card indicate that a particular service offers a certain functionality on behalf of the subscriber. The subscriber is responsible for the accuracy of the details on the services certificates; these were previously known as 'system cards'. A subscriber can have multiple services, and a service card can be requested for each of these services. The UZI-register guarantees the relationship to the subscriber. On services cards, the authenticity and confidentiality certificates are combined in a single certificate.

¹⁰ Section 76 of Book 6 of the Dutch Civil Code [*Burgerlijk Wetboek*] speaks of 'other persons'. In its communications, the UZI-register will use the term 'auxiliary persons'.

For the time being, cards for services will only be issued to subscribers which are healthcare institutions as intended in the Quality of Healthcare Institutions Act. The issue of these cards for subscribers who are individual practitioners is expected to commence in the near future.

4.4 Certificates

The holder of a key pair can be determined with the aid of a certificate. A certificate is an electronic document which links the identity of the holder of the key pair with that holder's public key. Data about the holder is included in the certificate for that purpose. The public key of the holder is also included in the certificate. A certificate is signed by the trusted party. The electronic signature of the UZI-register is appended to all UZI certificates. This signature indicates that the certificate and the related key pair were issued by the UZI-register and that the UZI-register guarantees that the details in the certificate are correct.

4.4.1 Certificate profile

The certificates to be issued by the UZI-register have been specially designed, within the framework of the government PKI, for application within the healthcare sector. This means that the certificates include a number of healthcare-specific elements.

For instance: at the request of the sector, there is space in the certificate for healthcare practitioners for a standardized role code to be included, which can serve as the basis for authorization. This will facilitate the arrangements for authorization in cases where inter-institutional communications are involved. The same applies to access to healthcare related data and to role-linked information (e.g. product information specifically for pharmacists can easily be restricted to that target group on the basis of the professional role code). The roles included in the UZI-register will be taken from the BIG Act. The legally protected title will be used for medical specialists. If the Minister designates new professional groups, the professional and possible specialist titles to be used for these groups will be defined and recorded.

In order to ensure compatibility with the current situation, the UZI-register's certificates will also include an AGB code or an AGB institution number. The AGB code is already in use to identify various parties in the healthcare sector and is widely used for expense claim purposes. The following table shows which details will be included in which UZI card:

Subscriber	Card type	AGB
Healthcare practitioner	Healthcare practitioner	AGB code healthcare practitioner
	Named employee	AGB code healthcare practitioner (subscriber)
	Non-specific employee	AGB code healthcare practitioner (subscriber)
	Services	AGB code healthcare practitioner (subscriber)
Healthcare institution	Healthcare practitioner	AGB code healthcare practitioner
	Named employee	AGB institution number (subscriber)
	Non-specific employee	AGB institution number (subscriber)
	Services	AGB institution number (subscriber)

Table 1: Relationship between UZI and AGB

4.4.2 CA model

UZI-register certificates will be signed by the issuing CA. The UZI-register has elected to adopt a model with one CSP CA with four sub-CAs. The certificates contain a reference to and the signature of the sub-CAs, as illustrated in the figure below.

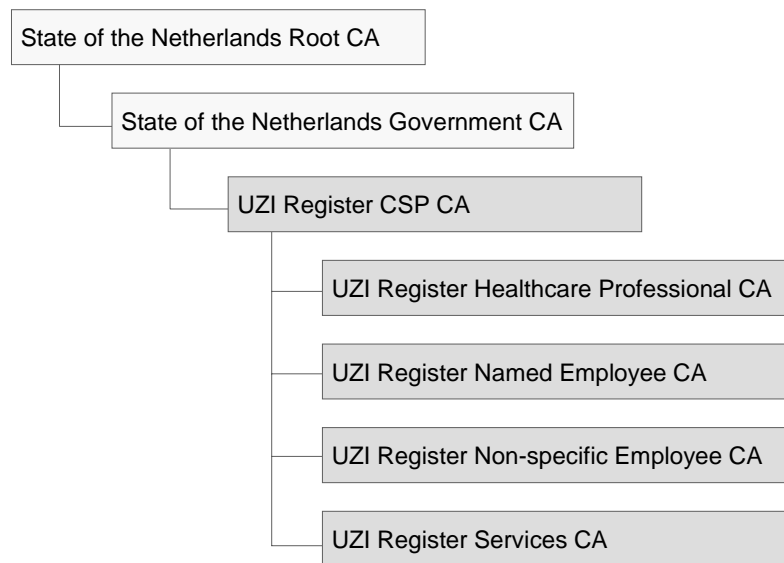


Figure 4: CA model of the UZI-register

4.5 Life cycle of UZI card

The products of the UZI-register are intended for the use of healthcare providers within the healthcare sector. A healthcare provider who/which wishes to obtain a UZI card must follow a number of steps. In addition, it is useful to consider a number of aspects involved in the actual use of the UZI card. The life cycle of the card is illustrated in the figure below and explained in more detail in the subsequent paragraphs.

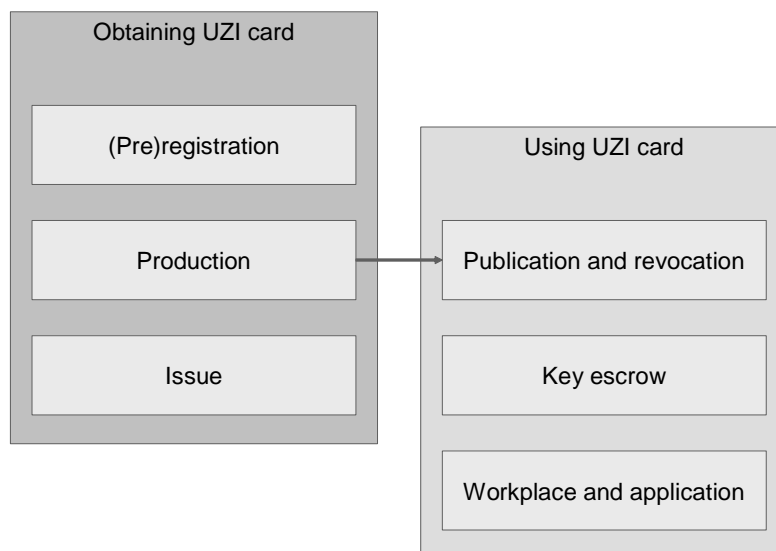


Figure 5: Life cycle of UZI card

4.5.1 (Pre)registration

A care provider can submit an application for registration as subscriber in the UZI-register via the Register's registration website. Subscribers who have already registered can also request UZI cards via the registration website.

On the basis of the details provided on the registration form, the UZI-register will carry out its initial checks. In the case of a healthcare institution, a check will be made that the institution is registered for that purpose with the Health Insurance Board. At the same time, a check will be made to ensure that the applicant is authorized to act on behalf of the institution. In the case of healthcare practitioners, as defined in Article 3 of the BIG Act, the UZI-register will check that this person is included in the BIG Register and ascertain whether or not he or she has been unconditionally suspended. For healthcare practitioners, as defined in Article 34 of the BIG Act, the UZI-register will check that this person is included in the Quality Register for Paramedics [*Kwaliteitsregister paramedic*]. Finally, the UZI-register will verify that any AGB code or AGB institution number given by the applicant is correct.

The UZI-register reports the findings of the various checks to the applicant. If the result of the checks is positive, the UZI-register will send the applicant a preprinted payment slip plus the necessary forms and the contract for signature. If the result of the checks is negative, the UZI-register will inform the applicant of the reasons why the request cannot be dealt with.

Upon return of the signed forms and the contract, the UZI-register will give instructions for the requested UZI card to be produced.

The procedure is slightly different for a service card. Before production commences, the applicant must report to the local post office so that an identity check can be carried out. Once the identity has been verified, the certificate can be produced and despatched.

4.5.2 Production

The key pairs are generated in a secure environment during production of the card. The public keys are incorporated in the certificate, and the certificates are signed by the appropriate sub-CA. The UZI-register only makes a back-up copy of the private keys which relate to the confidentiality certificates. Immediately after production of the keys and the certificates, the UZI-register publishes the certificates in the directory service.

An activation code (PIN code), an unlocking code (PUK code) and a cancellation code are generated for each card. All these codes consist of six digits. The card holder needs the PIN code to gain access to the UZI Card and to enable him to use the keys and certificates associated with it. If the card holder keys in the wrong PIN code three times, he will be locked out of the UZI card. The card can be rendered operational once more with the aid of the PUK code. If the wrong PUK code is keyed in three times, the card will be permanently locked. With the aid of the cancellation code, the card holder can have his card cancelled immediately via the website of the UZI-register at any time (24/7) in the event of theft or loss, or if he suspects it has otherwise been compromised.

The next step is to print the UZI card and to prepare the PIN mailer. The PIN mailer includes the PIN code, the PUK code and the cancellation code. The PIN mailer is sent to the intended card holder by post, and the UZI card is sent to the post office nominated by the applicant for collection.

4.5.3 Issue

The intended holder of the UZI card, or the applicant for a UZI card for non-specific employee, can collect the UZI card from the post office. The applicant can indicate which post office will be most convenient on the registration website.

On collection of the card, the applicant must present the collection slip and a valid proof of identification (in accordance with the Compulsory Identification Act [*Wet op de identificatieplicht*]). The post office will then carry out the necessary checks, based on the UZI card and the ID presented. The recipient must then sign the collection slip in exchange for the UZI card. The collection slip is also marked with the date and time of collection, so that both the recipient and the UZI-register have a record of the exact moment of issue.

4.5.4 *Publication and revocation*

Immediately after production, the certificates are published by the UZI-register. Relying parties can therefore make use of published certificates immediately (for verification purposes, for instance).

Besides new certificates, the UZI-register also publishes lists of withdrawn and cancelled certificates; these are known as Certificate Revocation Lists, or CRLs. Certificates can need to be revoked for a variety of reasons. Examples are:

- loss, theft, or mutilation of the carrier on which the certificate is stored (in this case, the UZI card);
- evident or suspected misuse;
- suspected compromise, because the card is lost, for example, or because the PIN and/or PUK code are no longer secure;
- permanent locking of the smart card (after an incorrect PUK code has been keyed in three times);
- when the healthcare institution ceases to exist;
- on termination of the holder's employment with the subscriber;
- inaccuracies in or changes to the data specified in the certificates;
- when the holder no longer fulfils the criteria for the status of healthcare institution or practitioner;
- when certified services are no longer used by the institution;
- when certified services are taken out of service.

When a holder submits a cancellation notice via the website, the UZI-register guarantees that the revocation will be published within four hours. If notices are submitted via other channels, a longer processing time may be applicable. A revoked certificate remains on the CRL until the expiry date of that certificate has passed.

The CRL should be consulted before a relying party depends on a certificate.

4.5.5 *Key escrow*

Data can be encrypted with the aid of the confidentiality key on the UZI card and hence rendered illegible for others for the purposes of transmission or storage. It is only with the aid of the private confidentiality key that this data can again be made legible. This means that if the UZI card is lost or stolen, it will no longer be possible - in principle - to render that data legible again. The UZI-register makes a back-up copy of the private keys which relate to the confidentiality certificates. This back-up is made in a secure environment and can only be accessed from the UZI-register by authorized persons.

The retrieval of a confidentiality key from the back-up is a strongly secured process. After all, only the holder himself may have access to this private key. The UZI-register advises those parties who make use of the confidentiality key to securely store data, that they should themselves take the necessary measures to ensure that they can access their data in the event of the key being lost.

4.5.6 *Workplace and application*

In order to actually use the UZI card, it is necessary that the applications are made suitable for the use of PKI technology. Guidelines for the adaptation of applications can be found on the government PKI website (www.pkioverheid.nl).

To facilitate their use, the UZI-register publishes the certificate profiles of the various types of UZI cards.

The UZI-register also recommends using a secure work station, which has at least one virus scanner and a firewall installed, or which is itself protected behind a firewall. Guidelines in this respect can be found on the UZI-register's website.

The work station of the card holder should also be equipped with a card reader and have the necessary software for this reader installed (middleware). The UZI-register indicates which combinations of card readers and software are guaranteed to work properly.

Appendix 1: Abbreviations and concepts

In the compilation of the definitions of concepts used in this paper, the following principles have been followed:

- Titles of Dutch legislation have been translated, but the original Dutch title is also given. Even where titles appear similar to existing legislation in other countries, differences in the legal systems will probably mean that the similarity is only superficial.
- In the case of PKI (Public Key Infrastructure) terminology, definitions follow those normally used in the government PKI and in specialist literature on this subject.

The glossary consists of three columns: Abbreviation, Concept and Definition. Entries have been sorted alphabetically by 'Concept'. In a number of cases, an explanation follows the definition, or an acknowledgement of the source of the information if applicable; in such cases a blank line is used to separate the information.

Abbreviation	Concept	Definition
AGB		see General Data Management Healthcare Practitioners
	Applicant	A healthcare practitioner or a representative of a (healthcare) institution, who is authorized by the legal representative of that institution to apply for the issue of UZI cards from the Registration Authority (RA) of the UZI-register on behalf of the (healthcare) institution.
	Authentication	A process by which a person's identity can be confirmed, or by which the integrity and origins of data can be checked and verified. See also: 'Authorization' and 'Identification'.
	Authorization	Giving a person the authority to carry out specific actions (examples include: insight into, modification and processing of data).
	BIG Register	Register of professional practitioners in individual healthcare, as intended in Articles 3 and 34 of the Individual Health Care Professions Act [<i>Beroepen in de Individuele Gezondheidszorg</i> (BIG Act)]. See also: www.big-register.nl
	Cancellation code	The code with which the card holder can submit and authorize a cancellation request in respect of a UZI card; to be used in the event of loss of the card, for example.
	Card holder	The natural person who makes use of the UZI card.
CIBG	Central Agency for Information on Healthcare Professions <i>Centraal Informatiepunt Beroepen in de Gezondheidszorg</i>	An agency of the Ministry of Public Health, Welfare & Sports, which is responsible for a number of statutory implementation tasks. See also: www.cibg.nl

	<p>Certificate</p> <ul style="list-style-type: none"> - public key certificate - electronic certificate 	<p>Electronic attestation which links data for the verification of particular person to data relating to the confidentiality and authenticity and/or electronic signature and thus confirms the identity of that person.</p> <p>A certificate is encrypted using the private key of the Certification Authority which issued the public key, so that the certificate cannot be forged.</p> <p>A certificate incorporates a range of characteristics, including:</p> <ul style="list-style-type: none"> a) an indication that the certificate is issued as a qualified certificate; b) the identification of the certification service provider and the country in which it is established; c) the name of the signatory; d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the qualified certificate is intended; e) signature-verification data which correspond to signature-creation data under the control of the signatory; f) an indication of the beginning and ending dates of the period of validity of the qualified certificate; g) the identity code of the qualified certificate; h) an electronic signature of the issuing certificate service provider which fulfils the criteria of paragraphs a through d of Section 15a(2) of Book 3 of the Dutch Civil Code [<i>Burgerlijk Wetboek</i>]; i) possible limitations on the scope of use of the certificate, if applicable; and j) possible limitations with regard to the value of transactions for which the qualified certificate can be used.
	Certificate holder	A natural person or legal entity for whose benefit a certificate is issued and whose identity can be verified with the aid of the certificate.
	Certificate profile	A description of the contents of a certificate. Each type of certificate (signature, confidentiality, etc.) has an individual design and therefore an individual description. The description also contains agreements about name designation etc.
CRL	Certificate Revocation List	<p>A list of revoked (i.e. withdrawn) certificates.</p> <p>This list is public, and can be consulted by anyone. The list is made available by and under the responsibility of the UZI-register. The CRL is itself electronically signed by the CA of the UZI-register.</p>
CA	Certification Authority	The component of the UZI-register which signs certificates and which is trusted by end users.
	Certification services	The issuance, management and revocation of certificates by certificate service providers, as well as other services which are connected with the use of electronic signatures, with identity and confidentiality.
CSP	Certification Service Provider	"certification-service-provider" means an entity or a legal or natural person who issues certificates and/or provides other services related to electronic signatures, including identity and confidentiality. The UZI-register is a CSP.

WID	Compulsory Identification Act <i>Wet op de identificatieplicht</i>	<p>The Compulsory Identification Act specifies the passport and the ID card as valid means of identification.</p> <p>A number of documents have been declared equivalent to the passport and ID card: diplomatic passport, service passport, travel documents for refugees or aliens and other travel documents nominated by the Minister, such as the Dutch ID card.</p> <p>The emergency passport and the 'laissez passer' do not quality as valid identification documents, nor does the driving licence.</p>
	Confidentiality	<p>The guarantee that data will actually and exclusively arrive at its intended and authorized destination, without the risk that anyone else can decipher that data. Outside the private sector, the term 'exclusivity' is also used.</p>
	Electronic signature	<p>A signature which consists of data in electronic form which are attached to or logically associated with other electronic data and which can be used as a method of authentication.</p> <p>The electronic signature which can be appended with the aid of the UZI card is known formally as an 'advanced electronic signature'. This is an electronic signature with the same force of law as a handwritten signature on paper, as long as it fulfils the following criteria:</p> <ul style="list-style-type: none"> • it is uniquely linked to the signatory; • it is capable of identifying the signatory; • it is created using means that the signatory can maintain under his sole control; • it is linked to the data to which it relates in such a manner that any subsequent change to that data is detectable; • it is based on a qualified certificate as intended in Article 1.1, paragraph ss* of the Dutch Telecommunications Act [<i>Telecommunicatiewet</i>]; • it is generated by a secure signature-creation device, as intended in Article 1.1, paragraph vv* of the Dutch Telecommunications Act. <p>Source: Electronic Signatures Act [<i>Wet Elektronische Handtekeningen</i>].</p> <p>* As from 8 July 2004, these components were renumbered in the named Act (ss was originally dd, and vv was gg).</p>
	Electronic identity	<p>A unique electronic representation of an identity, in the form of an X.500 Distinguished Name structure for example.</p> <p>This electronic data is added to, or linked in a logical way, to other electronic data. They act as a unique characteristic of the identity of the owner.</p>
	End user	See 'Card holder' and 'Relying party'.
	Escrow Key escrow	<p>Key security. A method of storing a copy of a private key, which is given into the custody of a trusted third party known as a Key Escrow Agency (KEA).</p> <p>If necessary, specifically authorized persons can obtain this copy; only the confidentiality key is given in escrow.</p>

AGB	General Data Management Healthcare Practitioners <i>Algemeen GegevensBeheerzorgverleners</i>	A database in which data about healthcare practitioners is stored. Alongside general information about the person and the practice, this registration also includes data which can be of importance in communications between healthcare providers and health insurers, particularly in the domain of expense claims. The AGB database is managed by Vektis.
	Healthcare	Healthcare is taken to mean all care which is defined by or pursuant to the Compulsory Health Insurance Act [<i>Ziekenfondswet</i>], the Exceptional Medical Expenses Act [<i>Algemene Wet Bijzondere Ziektekosten</i>], and by Orders in Council. Source: Quality of Healthcare Institutions Act.
	Healthcare institution	An organizational arrangement as intended in the Quality of Healthcare Institutions Act plus any other organizational arrangements as may be designated by the Minister for Public Health, Welfare & Sports.
	Healthcare insurer	National Health Insurance schemes, private health insurers or insurers governed by public law.
	Healthcare practitioner	A practitioner as intended in Article 3 or Article 34 of the BIG Act.
	Healthcare providers	Specific categories of healthcare practitioners and healthcare institutions as may be designated by the Minister for Public Health, Welfare & Sports.
	Hierarchy	A 'tree' illustrating the chain of trust between and among Certification Authorities (CAs).
	Identification	The process by which the identity of a person or an economic entity is determined.
OPTA	Independent Post & Telecommunications Authority <i>Onafhankelijke Post en Telecommunicatie Autoriteit</i>	OPTA is the watchdog organization for the postal and telecoms market in the Netherlands. OPTA stimulates competition in the markets for post and telecom services. Source: www.opta.nl
	Individual healthcare practitioner	An individual healthcare practitioner is someone who is not attached to a healthcare institution as intended in the Quality of Healthcare Institutions Act [<i>Kwaliteitswet Zorginstellingen</i>].
	Key(s)	See respectively: <ul style="list-style-type: none"> • Private key • Public key
NICTIZ	National ICT Institute for Healthcare <i>Nationaal ICT Instituut in de Zorg</i>	Many of the parties involved in the healthcare sector take part in this organization: providers of care (doctors, hospitals, etc.), consumers of care (patient associations), healthcare insurers and the government. NICTIZ's primary task is to create a national information system for and on behalf of the patient/client, making use of the latest developments in information technology. See also: www.nictiz.nl

	Non-repudiation <i>onweerlegbaarheid</i>	Non-repudiation provides proof of the origin or the receipt of data, so that neither party (neither recipient or originator) can deny the transaction or the message. In the case of the UZI-register, this feature is linked to the certificate for the electronic signature.
OPTA		see Independent Post & Telecommunications Authority
WBP	Personal Data Protection Act <i>Wet Bescherming Persoonsgegevens</i>	The most important rules for the recording and use of personal data are set out in the Dutch Personal Data Protection Act. This Act governs all usage or processing of personal data, from the collection thereof through to the destruction of personal data.
PIN	Personal Identification Number	The data that is needed to use a UZI card. This data is linked to the person and must be kept secret at all times. The UZI-register uses a PIN code as activation data.
	Personal key	See 'Private key'.
PUK	Personal Unblocking Key	The PUK code is needed to unlock the UZI card.
	PIN mailer	The PIN mailer contains the PIN, PUK and cancellation code and, depending on the type of card, is sent to the applicant or the card holder. The codes are printed in a special secure way so that only the person who opens the envelop can read the codes.
PA	Policy Authority	An authority under the responsibility of the Minister of the Interior and Kingdom Relations which determines the Certificate Policy (CP) of the UZI-register.
	Private key	The half of an asymmetric key pair which should be known only to the holder thereof, and must be kept strictly secret. The term secret or personal key is also used.
	Public key	The half of an asymmetric key pair which can be made known publicly. See also: 'Private key' and 'Public Key Infrastructure'
PKI	Public Key Infrastructure	A combination of architecture, technology, organization, procedures and regulations, based on asymmetric key pairs. The aim is to make it possible to carry out secure and reliable electronic communications and to offer reliable electronic services.
PKI-overheid	Government PKI	The government agency responsible for overseeing and regulating the PKI used for communications to and from government.
	Qualified certificate	A certificate which meets the requirements laid down in Article 18.15 (2) of the Dutch Telecommunications Act and is provided by a certification service provider that fulfils the requirements laid down in Article 18.15 (1) of that same Act.
KwZ	Quality of Healthcare Institutions Act <i>Kwaliteitswet Zorginstellingen</i>	The aim of the Quality of Healthcare Institutions Act is to guarantee the quality of care provided by healthcare institutions from the point of view of the State. The Act also sets out the obligations which must be fulfilled by such an institution.
	Review register	A register recognized by the Policy Authority of the UZI-register. The UZI-register can guarantee that a healthcare practitioner or institution which is included in such a register has the status of healthcare practitioner or healthcare institution.

	Revocation	<p>Revocation concerns the invalidation of a certificate.</p> <p>A certificate is revoked by publishing its serial number on the Certificate Revocation List (CRL) (revocation = withdraw, recall, rescind).</p>
	Relying party	The natural person or legal entity who is the recipient of a certificate and who acts in reliance on that certificate.
	Root certificate	This is the certificate belonging to the point where user confidence in all government PKI issued certificates has its origins. There is no higher level CA from which this trust can be derived. This certificate is signed by the holder itself, as the body responsible for the highest level trust point. All underlying or subordinate certificates are issued by the holder of the root certificate.
	Smart card	<p>A plastic card, the size of a credit card, in which is embedded an electronic chip which incorporates a microprocessor, memory storage and a power source.</p> <p>Such cards can be used to store information and are easy to carry around.</p>
	Subscriber	A natural person or an incorporated entity who/which concludes an agreement with the UZI-register by which this person/entity becomes a user of certification services.
	UZI card	The carrier of the electronic identity of a healthcare provider.
UZI	<p>Unique Healthcare Practitioner Identification</p> <p><i>Unieke Zorgverleners Identificatie</i></p>	A unique identification system for the healthcare providers.
	UZI-register	<p>A register of healthcare providers.</p> <p>The UZI-register ensures that all healthcare providers can be uniquely identified. The system is based on a PKI which links the legal and physical identity to an electronic identity and sets that identity out in certificates.</p> <p>See also: www.uzi-register.nl</p>
WBP		see Personal Data Protection Act
WID		see Compulsory Identification Act

Appendix 2: Related documentation

All documentation in Dutch unless otherwise stated - titles have been translated for convenience only.

Survey

- A review of the identification, authentication and authorization of healthcare practitioners, CIBG, June 2000

Definition study UZI-register

- Report on the preparatory phase of the definition study UZI-register, CIBG, version 1.0, April 2001
- Memorandum on results of definition study UZI-register, CIBG, version 1.0, dated 24 August 2001
- Investigation of the legal basis of the UZI-register, CIBG, version 1.0, dated 24 August 2001
- Certificate Policy for the UZI-register, CIBG, version 1.0, dated 24 August 2001
- Regulations Unique Healthcare Provider Identification Register, CIBG, version 1.0, dated 24 August 2001.
- Functional specifications for the definition study Unique Healthcare Provider Identification Register, Part 1 Corporate model, CIBG, version 1.0, dated 24 August 2001.
- Functional specifications for the definition study Unique Healthcare Provider Identification Register, Part 2 System specifications, CIBG, version 1.0, dated 24 August 2001.
- Scenarios for implementation and management of Unique Healthcare Provider Identification Register, CIBG, version 1.0, dated 24 August 2001.

UZI-register - supervised start-up

- Specifications for the European invitation to tender UZI-register, version 1.0, April 2004
- Advisory report: UZI domain and UZI number, version 1.0, dated 4 May 2004
- Advisory report: Implementation, highest level trust point and body responsible for policies, version 1.0, dated 18 June 2004
- Advisory report: Three certificate model, certificate profiles, infrastructure and certificate carriers, version 1.0, dated 29 September 2004
- Advisory report: PKI middleware and card readers, card portfolio, requirements for issuing process and design of LRAs, version 1.0, dated 25 November 2004

Appendix 3: Pilot projects

The practical testing of the UZI-register and the supervised start-up was carried out with the aid of the following pilot projects:

KSYOS - Teledermatology, email and web-based

As part of the KSYOS pilot project, use of the UZI card in the context of the email-based Teledermatological Consultation System in Drachten was evaluated. This application allows GPs to send digital photographs of their patients' skin disorders to the dermatologist by email, together with a standard information form. The dermatologist's answers can be expected within a few days. This answer can contain instructions for treatment by the GP or a recommendation for referral to the dermatologist. The UZI card was used to guarantee the security of patient data during such communications. The non-repudiation certificate, or electronic signature, was used for this purpose. Interviews with various GPs and dermatologists formed an integral part of the evaluation process.

Zorgring Zeeland - Trauma registration pilot scheme

In the pilot project entitled Zorgring Zeeland pilot scheme, UZI certificates were used and tested by future users; these included medical specialists, accident and emergency departments and hospital pharmacies. The pilot was actually a pre-evaluation of the use of UZI cards for the National Trauma Information System (NTIS), using only test environments. The aim is to achieve uniformity of trauma registration so that patients, GPs, medical specialists, hospital and local pharmacists can all make optimum use of the trauma registration scheme with the aid of ICT. Uniformity will make it possible to use data stored in the national trauma network (after consent has been obtained from the trauma specialist at the healthcare institution for example) for other purposes such as epidemiological research, trauma incidence analysis, comparisons with certain disorders, etc.

Trauma registration Brabant

This pilot project in the province of Brabant used the same application as the Zorgring Zeeland scheme did. In a test environment, medical staff at St. Elisabeth's Hospital in Tilburg had their first experience with the NTIS application and the functioning of the UZI card. The National Association of Trauma Specialists is currently investigating the necessity of using the UZI card to gain access to the application. It has been decided to offer the application nation-wide as from 1 January 2005; use of the UZI card will be optional.

VECOZO/Ring Amsterdam/National Association of General Practitioners (LHV) - 'verification of insurance eligibility' application

This pilot project was used to evaluate the use of UZI certificates in the verification of insurance eligibility application. With the aid of the verification of insurance eligibility application, healthcare practitioners who have signed a contract with VECOZO (an organization which promotes secure communication in the healthcare sector) can log in to the VECOZO site with the aid of their UZI card. Via the site the healthcare provider can then check whether or not a patient has health insurance. Interviews with GPs and a number of pharmacists formed part of the evaluation. A number of Apple users were also involved in this pilot.

VECOZO - MedDos

Besides the verification of eligibility application, the VECOZO pilot was also used to evaluate VECOZO's MedDos (= Medication Record) application.

This application allows healthcare practitioners to view medication data relating to a patient online via the internet. Requests for insight into records are dealt with via VECOZO. VECOZO then submits the request for the necessary details to the various healthcare insurers. In this instance, the details concern medication which has been or will be paid for by the healthcare insurers. A radiologist, a

hospital doctor and a pulmonary specialist from the Zeeuws Vlaanderen Hospital in Terneuzen were interviewed as part of the evaluation.

Appendix 4: Participants in consultation sessions

The following persons took part in one or more (pre)consultation sessions, or responded via the UZI-register's website (www.uzi-register.nl):

Mr. W.L. Posthumus	University Medical Centre
Mr. T.L.F. Urbanus	University Medical Centre, University of Amsterdam
Mr. L. Taal	Utrecht University Medical Centre
Mrs. H. Deijkers	Ambulance Zorg Nederland (federation of ambulance services)
Mr. W. H. Salzmann	Health Insurance Board (CvZ)
Mr. S. Corvers	Corvers Procurement Services B.V.
Mrs. A. Koppelmans	CZ Group, Healthcare insurance
Mrs. B. Augustijn-Vos Dordrecht/Gorinchem	District Specialisten Beraad West-Brabant/Zeeland &
Mr. P. Epping	Epping Consultancy
Mr. A.C. de Kok	Netherlands Foundation for Mental Health Care (GGZ)
Mr. P.J. Izeboud	Groene Land Achmea
Mr. B. Postma	Groene Land Achmea
Mr. R.C. Stadt	Royal Netherlands Association for Physiotherapy (KNGF)
Mr. J.D.L. Kroon	Royal Netherlands Society for the Advancement of Pharmacology (KNMP)
Mrs. J.A. Rendering	Royal Netherlands Society for the Advancement of Pharmacology (KNMP)
Mrs. L. Markenstein	Royal Netherlands Medical Society (KNMG)
Mr. S. Pippel	KSYOS Health Management Research
Mr. L. Witkamp	KSYOS Health Management Research
Mr. A.R. Esch	National Association of General Practitioners (LHV)
Mr. G. Fidder	Dutch National Association for Domiciliary Services (LVT)
Mr. C.P. Louwerse	Leiden University Medical Centre
Mr. H.B. Haveman	Ministry of Health, Welfare & Sports
Mrs. N. Kootker	Ministry of Health, Welfare & Sports
Mr. M. Rozeboom	National Society for the Advancement of Dentistry
Mr. E.C. Hermans	Dutch Federation of Patients and Consumers Organisations (NPCF)
Mrs. A. Nijhuis	Dutch Federation of Patients and Consumers Organisations (NPCF)
Mr. T.R. van Althuis	Dutch College of General Practitioners
Mrs. K.H. Njoo	Dutch College of General Practitioners
Mrs. N. Besseler	Netherlands Normalization Institute - Healthcare
Mrs. S. Golyardi	Netherlands Normalization Institute - Healthcare
Mr. T. Hooghiemstra	NICTIZ
Mr. F. van Dool	NICTIZ
Mr. P. van Gasselt	Association of organizations for ICT in the Healthcare sector
Mr. T. Tjee	Dutch Association of Medical Specialists
Mr. E. van Dongen	OZ Healthcare Insurance
Mr. E. Hardam	Government PKI
Mr. T. Behre	Government PKI
Mr. R. Brand	Government PKI
Mr. T. Gruter	RING Amsterdam
Mr. J.N. Hoogstraten	TNO Telecom
Mrs. L. Baaten	Brabant Trauma Centre

Mr. M. van Hulzen	Radboud Medical Centre, University of Nijmegen
Mr. T. Lont	Univé Insurance
Mr. W.R.A. de Jong	Vektis
Mr. F. van Bommel	Vektis
Mr. J. Janssens	Vektis
Mr. H. Wilson	Vektis
Mr. H. F. Prins	Association for the Care of the Handicapped in The Netherlands (VGN)
Mr. R.H.M. Bongers	Rivierenland Hospital
Mr. P. Jansen	Dutch Association of Health-care Insurers
Mr. C. de Jong	Dutch Association of Health-care Insurers

Appendix 5: Applicable standards

This appendix contains a summary of the standards with which the UZI-register complies. Where possible, the standards have been grouped around the components of the UZI-register to which they relate. A summary of standards, guidelines and legislation is then given for each group so formed.

Certification and legal framework

ETSI TS 101 456 v1.2.1 (2002-04), Policy requirements for certification authority issuing qualified certificates.

Schedule of requirements from the PKI for the government, www.pkioverheid.nl:

- SoR part 2b Certificate Policy - Government domain, version 5.0, September 2003
- SoR part 2d Certificate Policy - Services, appendix to CP Business and CP Government, version 2.0, September 2003

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. These guidelines were implemented in the Dutch Electronic Signatures Act [*Wet elektronische handtekeningen*] on 8 May 2003.

Dutch Electronic Signatures Act [*Wet elektronische handtekeningen*], the Act of 8 May 2003 modifying Book 3 and Book 6 of the Dutch Civil Code [*Burgerlijk Wetboek*], the Telecommunications Act [*Telecommunicatiewet*] and the Economic Offences Act relating to Electronic Signatures [*Wet op de economische delicten inzake elektronische handtekeningen*] in the context of the implementation of Directive 1999/93/EC of the European Parliament and the Council of the European Union of 13 December 1999 on a Community Framework for Electronic Signatures (OJ EC L13) (Electronic Signatures Act), www.overheid.nl.

Electronic Administrative Communications Act, an act of 29 April 2004 which comprises a supplement to the General Administrative Law Act [*Algemene wet bestuursrecht*] and sets out the rules for electronic communications between citizens and government bodies; this act also prompts the amendment of various other legislation.

Individual Healthcare Professions Act [*Wet Beroepen in de individuele Gezondheidszorg Wet*, BIG Act], law passed on 11 November 1993, which sets down rules on the provision of healthcare services by professional practitioners, www.overheid.nl.

Quality of Healthcare Institutions Act [*Kwaliteitswet zorginstellingen*, KwZ], law passed on 18 January 1996 which regulates the quality of healthcare institutions, www.overheid.nl. Article 1 of this Act defines a "healthcare institution" as a hierarchical arrangement for the purpose of providing healthcare services.

Smart card

The UZI-register has opted for the following smart card:

Smart card features	Specifications
Microprocessor:	Philips P8WE5033; 32 k Eeprom
Operating system:	IBM JCOP 21 id
Manufacturer:	Trüb

The smart card (a combination of a microprocessor and an operating system) has been independently certified in accordance with the following standards:

- [Common Criteria EAL4+] : Common Criteria for Security Evaluation (Version 2.1, ISO/IEC 15408: 1999), Evaluation Assurance Level 4+ (EAL4+), <http://www.commoncriteriaportal.org/>
- [FIPS 140-2 level 3] : Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, <http://csrc.nist.gov>

According to independent testing, the smart card hardware (Philips P8WE5033; 32 k Eeprom, Triple-DES coprocessor, FameX RSA coprocessor) complies with the following standards:

- Supply voltage: tests indicate that the card functions properly with a supply voltage of both 5V and 3V.
- [ISO7816-1 t/m 3] Information technology - Identification cards - Integrated circuit(s) cards with contacts:
 - Part 1: Physical characteristics
 - Part 2: Dimensions and location of contacts
 - Part 3: Electronic signals and transmission protocols
- [ISO/IEC 7816-3 Amd. 1] This is an asynchronous, half-duplex smart card communications protocol, generally known as the T=1 protocol.

The smart card uses [IBM JCOP 21 id] as its Card Operating System, a system which is based on open standards.

- [JCOP 21 id] is an IBM implementation of the [JavaCard 2.1.1] and the [GlobalPlatform Card Specification v2.1.1] basic specifications. Further information is available via www.ibm.com, key search words 'JCOP21id Technical Brief'.
- [Java Card v2.1.1] : JavaCard specifications from Sun: <http://java.sun.com/products/javacard/>.
- [GlobalPlatform Card Specification v2.1.1] : GlobalPlatform Card Specification v2.1.1 - published March 2003, <http://www.globalplatform.org/>.
- [ISO7816-1 t/m 3] Information technology - Identification cards - Integrated circuit(s) cards with contacts:
 - Part 4: Interindustry commands for interchange
 - Part 8: Commands for security operations
- [PKCS #15 v1.1] : Cryptographic Token Information Syntax Standard (6 June 2000) , RSA Laboratories, www.rsasecurity.com.

Card reader

The UZI-register has subjected the following card readers to interoperability tests.

Product	Specifications
Readers, Omnikey	CardMan 3121 USB
Readers, Omnikey	CardMan 4040 PCMCIA
Gemplus	GemPC TWIN USB
Gemplus	GemPC 400 (PCMCIA)

Note: In principle, the selected PKI Middleware worked satisfactorily with all [PC/SC v1.0] compliant card readers. However, in an endeavour to avoid problems, the reader must have be capable of producing 60mA.

Standards supported for the card reader

- [PCMCIA] : PC Card standard, developed by the Personal Computer Memory Card International Association, <http://www.pcmcia.org>
- [PC/SC v1.0] : Personal Computer/Smart Card interface specifications, <http://www.pcscworkgroup.com/>
- [USB] : Universal Serial Bus, www.usb.org

PKI middleware

The UZI-register has opted for SafeSign (www.aeteurope.com) as PKI middleware. The following versions of PKI middleware have been tested by the UZI-register in regard to interoperability with card readers and smart card.

Product	Specifications
PKI middleware AET	SafeSign version 2.0.14 (for the Windows platform)
PKI middleware AET	SafeSign version 2.0.14 for MacOS X
PKI middleware AET	SafeSign version 2.0.x for Linux

There are two standards which relate to the applications which make use of SafeSign:

- [CryptoAPI] : Microsoft Crypto API, www.microsoft.com
- [PKCS#11] : Public-Key Cryptography Standards. PKCS #10 v2.11: Cryptographic Token Interface Standard, RSA Laboratories, www.rsasecurity.com.

In addition, SafeSign also supports the following standard:

- [PKCS#12] : Personal Information Exchange Syntax v1.0, RSA Laboratories, www.rsasecurity.com.

Dissemination Service

Certificates and CRLs can be called up using the [HTTP] protocol. [SSL] is used to secure this protocol and also communications with the directory service (LDAP).

- [HTTP]: RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, www.ietf.org.
- [SSL]: SSL3.0 Specification, www.netscape.com

The LDAP directory service meets the following standards:

- [X.509v3] : ISO/IEC 9594-8, 4th edition, 2002 (=ITU-T Rec. X.509): Information Technology – Open Systems Interconnection – The directory: Public-key and attribute certificate framework
- [X.520] : ITU/X.520 Attribute types
- [X.521] : ITU/X.521 Object Classes
- [RFC 2798] : IETF/RFC 2798, Definition of the inetOrgPerson LDAP Object Class
- [RFC 2119] : IETF/RFC 2119, Lightweight Directory Access Protocol (v3)

OCSP services which will comply with the following standard are currently in preparation:

- [RFC 2560]: Online Certificate Status Protocol – OCSP, <http://www.ietf.org/>

Certificate and CRL profiles

The profiles meet the following standards:

- [X.509v3] : ISO/IEC 9594-8, 4th edition, 2002 (=ITU-T Rec. X.509): Information Technology – Open Systems Interconnection – The directory: Public-key and attribute certificate framework
- [ISO8825] : ISO/IEC 8825-1: 1995 Information technology - ASN.1 encoding rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- [RFC3280] : Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile, April 2002
- [RFC2279] : UTF-8, a transformation format of ISO 10646, January 1998

Signature certificates classify as what are known as qualified certificates and accordingly comply with the following additional standards:

- [ETSI 101 862] : ETSI TS 101 862 - Qualified Certificate Profile
- [RFC3739] : Internet X.509 Public Key Infrastructure Qualified Certificates Profile, March 2004

Cryptographic Algorithms

All the cryptographic algorithms used for the UZI-register comply with [ETSI SR 002 176]. Algorithms and Parameters for Secure Electronic Signatures, v1.1.1 (2003-03)

- [ETSI SR 002 176] only describes the algorithms for electronic signature and not the trust function (by encrypting messages) and authenticity. The same algorithms as are used for the electronic signature are also used for authentication. Symmetric algorithms which are not included in [ETSI SR 002 176] are often used to encrypt messages. For that reason, and until standardization has been achieved at European level, the [3DES] and [AES] variants have been chosen.
- [3DES] : Triple-DES, defined in the Federal Information Processing Standards Publication 46-3, Data Encryption Standard, National Institute of Standards and Technology, <http://csrc.nist.gov>, and in the standard ANSI X.9.52 'Triple Data Encryption Algorithm Modes of Operation' (American Bankers Association, 1998).
- [AES] : Advanced Encryption Standard, Federal Information Processing Standards Publication 197, <http://csrc.nist.gov>.

In the context of the permitted algorithms, it has been decided to further opt for:

- PKCS #1 V1.5: Nov. 1993, V2.0: July, 1998
- V2.1 June 2002: RSA Cryptography Standard, RSA Laboratories, www.rsasecurity.com.
- [SHA-1] : Federal Information Processing Standards Publication 180-1, 1995 April 17, Secure Hash Standard.

RSA keys with a length of 1024 bits are used for users; the RSA keys of CAs have a length of 2048 bits.

Registration system

[PKCS#10] is used for requesting services certificates.

- Public-Key Cryptography Standards. PKCS #10 v1.7: Certification Request Syntax Standard, RSA Laboratories, www.rsasecurity.com.