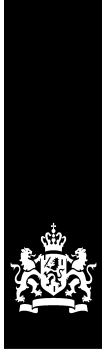

CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Certification Practice Statement (CPS)

Version 11.4

Date 21-06-2022
Status Final(UZ52.01)

Contents

List of tables

List of figures

Revision history

Table 1 Revision history

Version	Date	Status	Comment
1.0	17/01/2005	Final	
2.0	11/01/2006	Final	
3.0	01/03/2007	Final	
4.0	01/06/2008	Final	
4.1	01/10/2008	Final	
5.0	18/01/2012	Final	
6.0	01/04/2016	Final	
7.0	01/06/2017	Final	
8.0	04-01-2018	Final	- The Private G1 hierarchy of the State of the Netherlands release - Article 15 eIDAS
9.0	22-03-2018	Final	- The Public G3 hierarchy of the State of the Netherlands release
9.1	10-09-2018	Final	- Textual changes and clarifications - Change regarding Time required to process a revocation request modified (par. 4.10.5) - Physician Assistant added to article 3 of het Individual Health Care Professions Act [Wet op de beroepen in de individuele gezondheidszorg] (Wet BIG) - Limited liability with regard to the delivery of the UZI card added - Change regarding definition of care - General Data Protection Regulation (De Algemene verordening gegevensbescherming) - Retention periods included (par. 5.5.2) - Change procedure modified (par. 9.12)
9.2	04-11-2018	Final	- The 'employee card not in name' available.
9.3	23-11-2018	Final	- Textual changes and clarifications - The G2 hierarchy added - Reference to section 3.2.2.4. of the Baseline Requirements included. - Chapter 8 'Conformity assessment' updated
9.4	01-06-2019	Final	- Textual changes and clarifications - Right to check on compensating measures added (section 4.6.1.) - Update CaIssuer URL's after resigning of G3 CA's (par. 7.1.2)
9.5	01-08-2019	Final	- The UZI register will no longer withdraw old certificates 7 days after the renewed certificates have been issued.
9.6	01-11-2019	Final	- Reference to section 3.2.2.4.2, 3.2.2.4.6 and 3.2.2.4.7 of the Baseline Requirements (3.2.3). - G2 hierarchy for server certificates removed

9.7	01-12-2019	Final	- Office hours added for revocation requests (par. 4.10.5) - Orthopedagoog-generalist (role code 31) added to attachment 3
9.8	01-04-2020	Final	- Chapter 9 'general terms en clarifications' updated and textual changes and clarifications. - X-pact changed to Cannock Outsourcing B.V. - Confirmation Server certificate removed - Reference to RFC 2560 changed to IETF RFC 6960 - registered dental hygienists [geregistreerd-mondhygiënisten] (role code 79) added to Annex 3. - Reference to section 3.2.2.4.6 changed to 3.2.2.4.18 of the Baseline Requirements.
9.9	01-05-2020	Final	- Contact details [phone number] changed.
10.0	05-06-2020	Final	- UZI card delivery only possible within the Netherlands. - Data exchange with VZVZ regarding connection LSP
10.1	01-11-2020	Final	- Revoked certificates remain on the CRL after expiration date - General update on annex 3 and added specialism - Nurse specialist somatic Health care (076) - G21/G2 hierarchy removed.
10.2	01-12-2020	Final	- Adjustments following policy decision: Pharmacy assistants can no longer be registered as a care provider subscriber.
10.3	18-1-2021	Final	- Chapter 6 on technical security updated on Qualified. - Signature Creating Device: user activation is now required and certification status shall be monitored.
10.4	24-5-2021	Final	- Section 4.9 Revocation and suspension of certificates updated
11.0	20-9-2021	Final	- General review. - Subsection index in accordance with RFC3647. - Change in courier service Dynalogic → AMP Groep - Certificate acceptance; agreement with terms and conditions as stated in this CPS
11.1	17-12-2021	Final	- Change Wtzi to Wtza - General review.
11.2	01-03-2022	Final	- Specification of retention periods - Reference EUTL trustlist - Deviations from field lengths in RFC 5280 listed
11.3	02-06-2022	Final	- Change in representations and warranties - Removal Bachelor medical Assistant
11.4	21-06-2022	Final	- Expansion DAF

Accord TSP Management
Version: 11.4
Date: 20-06-2022

1 Introduction

1.1 Overview

1.1.1 Introduction to the UZI register

In order to facilitate the safe communication and consultation of confidential information in the care sector, three domains have been distinguished: the care consumers, the care insurers and the care providers. The Unique Healthcare Provider Identification Register (the so-called UZI register) is the register of care providers designated by the Minister of Health, Welfare and Sport as referred to in Article 14 of the Act Additional provisions for the processing of personal data in the care [Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg]. The UZI register is the certificate service provider (TSP)[1] that issues certificates for the unique identification and authentication of care providers and indication bodies in the care sector.

The aim of the UZI register is to identify care providers and indication bodies uniquely in the context of electronic communication and access to details. With this in mind the UZI register uniquely links the physical identity to an electronic identity and records these in certificates. The certificates and the accompanying cryptographic keys are located on a smart card[2]. In general terms, this is referred to as the UZI card in this Certification Practice Statement (CPS)[3].

The UZI register issues UZI cards to parties designated by the Minister of Health, Welfare and Sport based on legislation and regulations. A more detailed description of the user community of the UZI register is included in section 1.3 'Parties involved'. The UZI register issues certificates for the government under the PKI hierarchy[4].

The UZI-register makes online services available, such as the content on the website, the online revocation page and the digital application facility accessible to persons with a disability, wherever possible[5]. hereby, changes to the aforementioned online services will be tested against ETSI EN 301 549.

1.1.2 Types of cards and certificates

The UZI register issues various types of cards and certificates. *Figure 1 Cards model and certificates* provides a diagrammatic overview of the types of cards and the certificates per card type. The various types of cards are briefly clarified below.

[1] For an explanation of the terms and abbreviations used, please refer to Annex 1 which is entitled 'Definitions and abbreviations'.

[2] It relates to a so-called Qualified Signature Creation Device (QSCD)

[3] The term UZI card is used to refer to the certificates, keys and the corresponding bearer. [4.] Artikel 15 eIDAS

4 https://www.logius.nl/diensten/PKIoverheid/

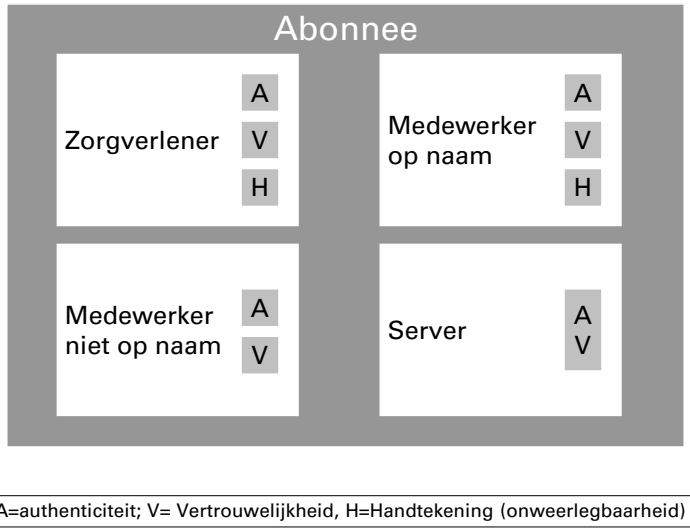

Figure 1 Cards model and certificates

Abonnee	Subscriber
Zorgverlener	Care provider [zorgverlener]
Medewerker niet op naam	Unnamed Employee [medewerker niet op naam]
Medewerker op naam	Named Employee [medewerker op naam]
Server	Server
A	A
V	C
H	S
A=authenticiteit	A=Authenticity
V=Vertrouwelijkheid	C=Confidentiality
H=Handtekening (onweerlegbaarheid)	S=Signature (non-repudiation)

Care provider card [zorgverlenerpas]
The care provider card [zorgverlenerpas] is for a professional as referred to in Articles 3 and 34 of the Individual Health Care Professions Act [Wet op de beroepen in de individuele gezondheidszorg] (Wet BIG). The UZI card is issued on the basis of a face-to-face check and check of the legal identity, after a check has taken place to establish whether the intended cardholder actually is a care provider (see Annex 2). In addition to the identity, the UZI register also guarantees the 'care provider status' and the relationship to the subscriber[6]. Care providers receive a personalised card and three certificates and key pairs (authentication, confidentiality and non-repudiation).

Named employee card [medewerkerpas op naam]
An employee of a subscriber of the UZI register can receive an 'named employee card ' [medewerkerpas op naam]. The card is issued on the basis of a face-to-face check and check of the legal identity of the certificate holder following a request by an authorised applicant. In addition to the identity, the UZI register also guarantees the relationship to the subscriber. Employees receive a personalised card and three certificates and key pairs (authentication, confidentiality and non-repudiation).

6 The UZI register guarantees the relationship to the subscriber by establishing that the legal representative, or a person authorised by the legal representative, has requested the card for the cardholder or certificate holder.

Unnamed employee card [medewerkerpas niet op naam]

An unnamed employee card cannot be obtained by a group of employees with a certain position as subscriber to the UZI register. The certificates of this UZI card indicate that the certificate holder is an official of the subscriber referred to in the certificates but cannot be directly traced back to a person. The UZI register guarantees the relationship to the subscriber and issues the card after a face-to-face check and check of the legal identity of the authorised applicant. For the 'unnamed employee card' [medewerkerpas niet op naam] the applicant also fulfils the role of certificate manager and is responsible for, among other things, registering the relationship to the specific employee(s) who are using the card. The 'unnamed employee card' [medewerkerpas niet op naam] is a non-personalised UZI card with two certificates and key pairs (authentication and confidentiality).
This UZI card cannot be issued under a subscriber care provider registration.

Server Certificates
Server certificates can be obtained for a subscriber's systems. These certificates indicate that a system exchanges details and/or offers services on behalf of the subscriber. The subscriber is responsible for the accuracy of the details in the server certificates of his systems. The UZI register guarantees the relationship to the subscriber and issues the server certificate after a face-to-face check and check of the legal identity of the applicant. For a server certificate the applicant also fulfils the role of certificate manager and is therefore responsible, on behalf of the subscriber, for the operational management of the certificate. In the case of server certificates, the authenticity and confidentiality certificate are combined into a single certificate.

1.1.3 CA model

Certificates which are issued by the UZI register have been signed by the UZI register. With this in mind the signature of the Certification Authority (CA) of the UZI register is used. The UZI register has a number of CAs. The relationship between these CAs is outlined below and in *Figure 2 CA-model Public G3/Private G1 generation*.

Public G3/Private G1 generation
The UZI register issues

1. UZI-card certificates under the public Root CA G3 of PKIoverheid (Public G3)
2. Server certificates under the private Root CA G1 of PKIoverheid (Private G1)

The figure below shows the CA model for the generation Public G3 / Private G1.
For completeness, the different types of end-user certificates are also included:

- AUT: Authenticity certificate ;
- VRT: Confidentiality certificate;
- HND: Signature certificate (non-repudiation certificate);
- S: Server certificate (combined authentication and confidentiality)

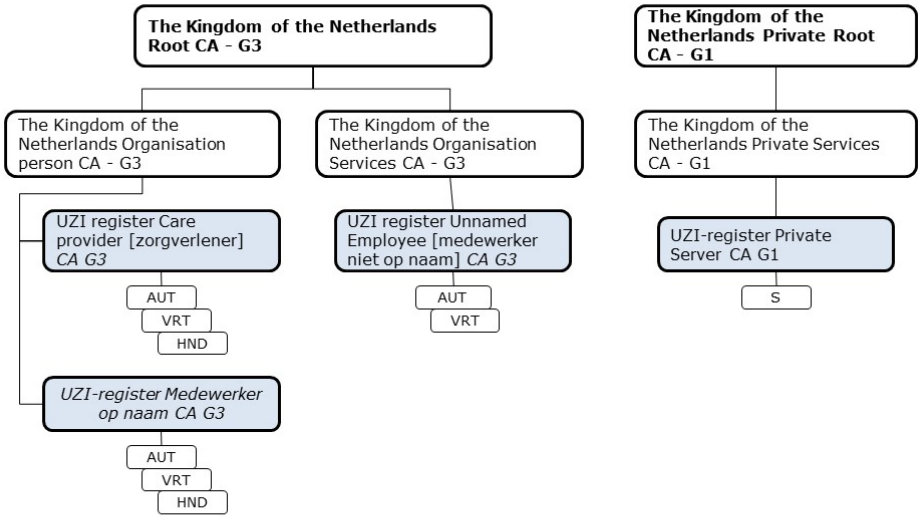

Figure 2 CA-model Public G3/Private G1 generation

1.2 Document name and identification

1.2.1 Purpose of the CPS

The CPS of the UZI register describes how the services are interpreted. The CPS describes the processes, procedures and control measures for applying for, producing, issuing, managing and retracting of the certificates. The parties involved can use this CPS to determine their confidence in the services provided by the UZI register. The general framework of this CPS is based on the model as presented in Request for Comments 3647. The RFC 3647 applies internationally as the de facto standard.

1.2.2 Relationship CP and CPS

This CPS describes how the requirements in the Certificate Policies (CPs) have to be interpreted. The CPs contain descriptions of which requirements are being imposed on the services. The CPS describes how these requirements have been interpreted. Table 12 Overview of certificates with OID of applicable CP Public G3/Private G1 generation indicate in which PKIoverheid domain the different types of cards and certificates are issued and which part of the Program of Requirements of PKIoverheid contains the CP.

1.2.3 Name and references

This document is formally referred to as a 'Certification Practice Statement (CPS)', abbreviated to CPS. A paper version of the CPS can be obtained from the contact address included in section 1.5.2.

The references to the CPS are included in the table below.

Table 2 CPS references

CPS	Description
Naming	Certification Practice Statement, UZI-register vX.xx
Link	https://www.zorgcsp.nl/cps/uzi-register.html
Object Identifier (OID)	2.16.528.1.1007.1.1

1.3 PKI Participants

The parties involved in the UZI register are the following:

- organisation that implements the UZI register, including suppliers of products and services;
- user community consisting of:
  - subscribers;
  - certificate holders/certificate managers;
  - trusting parties.

The CIBG fulfils the role of **TSP** and has final responsibility for supplying the certification services. The CIBG is an implementing body of the Ministry of Health, Welfare and Sport. The CIBG, in the role of TSP, is referred to in the rest of this CPS as 'the UZI register'.

Clauses about liability and guarantees of the TSP are included in sections 9.5, 9.5.1, 9.5.2 and 9.5.3.

1.3.1 Certification Authorities (CA)

The CA produces and publishes certificates and certificate revocation lists (CRLs). The CA arranges the production and publication of requested certificates on the basis of an authenticated request from the RA. Certificates are published directly after they have been created by the CA. Certificates are published on a CRL after the CA has received a message of revocation of the certificate from an authorised person. After revocation, the CA publishes the unique certificate serial numbers on the CRL in question. The CIBG has outsourced the role of CA to KPN B.V. . Multipost Services B.V. produces the UZI cards on behalf of KPN B.V.

1.3.2 Registration Authorities (RA)

The RA arranges the processing of certificate applications and all corresponding tasks. The RA physically collects the identification details, checks and registers these and carries out the verification checks described. After the checks, the RA instructs the CA to produce the UZI cards and publish the certificates. The CIBG fulfils the role of RA. The CIBG has subcontracted redistribution and issue of the UZI cards to KPN B.V. AMP Groep issues the UZI card on behalf of KPN B.V. after the identity of the certificate holder has been verified. AMP Groep also checks the identity of certificate managers.

1.3.3 Subscribers

The subscriber is the party on whose behalf the certificate holder acts when using the certificates.

The UZI register has two types of subscribers, namely people (care provider working alone) and organisations (institutions and indication bodies). Organisations and people that fulfil the criteria described in Annex 2 can register as subscriber of the UZI register. Only subscribers can apply for UZI certificates. If a subscriber is a care provider acting alone and has applied for the card for himself, this care provider will also be the certificate holder. The method of registration is described in Chapter 3 ("Identification and authentication).

1.3.4 Relying parties

A trusting party is the party that acts in confidence on a certificate for the possible purposes of authenticating care providers, verifying an electronic signature or encrypting communication with the party in question.

1.3.5 Other participants

Other participants include the certificate holders and certificate managers. A certificate holder is a natural person who is characterised in the certificate as the holder of the private key which is linked to the public key included in the certificate. For server certificates, no certificate holder is, in effect, included in the certificate. The applicant of the server certificate also fulfils the role of certificate manager. The certificate manager is related to the subscriber included in the certificate and carries out activities relating to the server certificate on behalf of the subscriber. The subscriber instructs the certificate manager to carry out the activities in question and records these in a proof of certificate management.

The obligations which are applicable to certificate holders and certificate managers are included in CPS sections 4.5.1

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The field of application of certificates issued by the UZI register is limited to the user community as described in section 2.3, section 3a of the Programme of Requirements of the PKI for the government. This user community consists of subscribers of the UZI register, certificate holders that belong to these subscribers and trusting parties.

The products of the UZI register are intended for care providers and indication bodies in the context of electronic communication and access to details. The applicability of the certificates is detailed in Table 3 Field of application of certificates.

Table 3 Field of application of certificates

Type of certificate	Purpose
Authenticity certificate	This certificate is used to authenticate the certificate holder and/or subscriber.
Confidentiality certificate	This certificate is used to encrypt the communication with the certificate holder of the care institution.
Signature certificate (non-repudiation certificate)	This certificate is used to verify an electronic signature by the certificate holder.
Server certificate (combined authentication and confidentiality)	This certificate is used for the authentication of systems and to protect communication.

1.4.2 Prohibited certificate uses

Certificates may only be used for the purpose indicated. Otherwise there are no restrictions on the use of the certificates.

1.5 Policy administration

1.5.1 Organization administering the document

CIBG manages the document.

1.5.2 Contact person

Information about this CPS or the services of the UZI register can be obtained via the contact details shown below. Comments on this CPS can be sent to the same address.

UZI register contact details:

Rijnstraat 50 Postbus 16114
2515 XP Den Haag 2500 BC Den Haag
Tel: 070 340 60 20
info@uzi-register.nl https://www.uziregister.nl/

The CA SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA SHALL publicly disclose the instructions through a readily accessible online means and in Section 1.5.2 of their CPS.

Suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates can be reported by e-mail at info@uzi-register.nl.

1.5.3 Person determining CPS suitability for the policy

Determining the suitability of the CPS policy is part of the CPS approval procedure, as assessed by an independent auditor.

1.5.4 CPS approval procedures

The UZI register is entitled to amend or supplement the CPS. Amendments apply as from the moment that the new CPS is published. The TSP management is responsible for correct compliance with the procedure as described in section 9.12 and for the eventual approval of the CPS in accordance with this procedure.

1.6 Definitions and abbreviations

For an overview of the definitions and abbreviations used, please refer to Annex 1.

2 Publication and Repository Responsibilities

2.1 Repositories

The UZI register publishes certificates, as part of the issue procedure. Trusting parties, certificate holders and subscribers can consult certificates via the directory service.

The directory service is adequately secured against manipulation and can be accessed online. Information about the status of a certificate can be consulted twenty-four hours a day and seven days a week by means of a Certificate Revocation List (CRL).

The UZI register is responsible for the website on which, among other things, this CPS is published. The CRL is also placed on this website (generated by the CA). This website also contains the online revocation page and provides a public search function for certificates.

2.2 Publication of certification information

The UZI register publishes TSP information on www.uzi-register.nl and www.zorgcsp.nl. Among other things, the locations offers access to the following documents and services:

- CPS,
- Certificate Revocation Lists (CRLs),
- TSP and CA certificates,
- Directory service (LDAP search page).

2.3 Time or frequency of publication

Certificates are published as part of the issue process. The CRL issue frequency is every hour.

2.4 Access controls on repositories

Published information is public in nature and freely accessible. The published information can be consulted twenty-four hours a day and seven days per week.

The published certificates can only be accessed publicly via the search function on the website.

3 Identification and Authentication

3.1 Naming

This paragraph describes how the certificate managers are identified and authenticated during the initial registration procedure and which criteria the UZI register imposes with regard to the names.

3.1.1 Types of names

All certificates issued by the UZI register have a 'subject' field (DistinguishedName) in which the holder's name can be found. This field consists of (X.500) attributes and is filled as follows:

Table 4 Name of certificate holder in UZI certificates (subject.DistinguishedName)

Attribute	**Care provider [zorgverlener]**	**Named employee [medewerker op naam]**	**Unnamed employee [medewerker niet op naam]**	**Server**
Country (C)	'NL'	'NL'	'NL'	'NL'
Organization (O)	Subscriber's name	Subscriber's name	Subscriber's name	Subscriber's name
OrganizationalUnit (OU)	(field missing for this card type)	(field missing for this card type)	Department	Department (optional)
Title (T)	Title of address of care provider (professional title, qualification title or specialism)	Not applicable	Not applicable	Not applicable
givenName (G)	First names	First names	Not applicable	Not applicable
surname (SN)	prefix and birth name of care provider	prefix and birth name of employee	Not applicable	Not applicable
CommonName (CN)	First names, surname prefix and birth name of care provider	First names, surname prefix and birth name of employee	Name of employee's position	System name
SerialNumber	UZI number	UZI number	UZI number	UZI number

Names of people included in the Certificate comply with the name format as defined in 'NEN 1888:2002 (nl), General personal details; Definitions, character sets and exchange formats' of the NEN.

No attributes are used other than those indicated above. A clarification of the other parts of the certificates is included in chapter 7.

3.1.2 Need for names to be meaningful

The name used in the issued certificates is unambiguous in such a way that is possible for the trusting party to establish irrefutably the identity of the certificate holder or subscriber.

3.1.3 Anonymity or pseudonymity of subscribers

The UZI register does not allow the usage of pseudonyms in the subscriber registration or card applications.

3.1.4 Rules for interpreting various name forms

The following points are relevant for the interpretation of the name:

- For care providers [zorgverlener] and named employees [medewerkers op naam], the commonName contains the birth name including prefixes and first names and title of nobility, as included in the identification document from the Persons Database [Basisregistratie Personen] (BRP) submitted with the registration. The commonName refers to the title of nobility in accordance with the identification document submitted upon registration. The valid identification documents are those referred to in Article 1 of the Compulsory Identification Act [Wet op de identificatieplicht] (WID). All first names must be written out in full on the submitted identification document.
- In principle, the commonName refers to all the first names in full in accordance with the Persons Database (BRP) or the identification document submitted upon registration. If the resulting commonName contains more characters than is technically possible, one or more first names will be replaced by initials, starting with the last full first name, and continuing until the resulting commonName does fit.
- In the case of an institution, the subscriber's name will contain the name as shown on the document submitted upon registration in order to identify the organisation. If the subscriber is a care provider working alone, the commonName of the care provider working alone will be included.
- The employee job name may not contain any name which is (wholly or partially) equal to, similar to, or gives the impression of a protected professional title, qualification title or specialism. The UZI register has drawn up a list of job names, from which a choice can be made. These are: administrative employee [administratief medewerk(st)er], assistant [assistent(e)], healthcare assistant [doktersassistent(e)], manager, employee [medewerk(st)er], trainee [stagiair(e)], dentist's assistant [tandartsassistent(e)]. It is not possible to submit a self-chosen job name.
- Department contains the department name given by the subscriber. The UZI register also imposes the requirement that the department name may not contain any name which is (wholly or partially) equal to, similar to, all gives the impression of a protected professional title, qualification title or specialism. A list of protected professional titles, qualification titles and specialisms is included in Annex 3 of the CPS. An assessment will take place on, for example, the basis of this overview. No assessment will take place with regard to spelling and writing errors.
- System name (also referred to as full domain name) contains the fully qualified domain name (FQDN) of the system.

All names are, in principle, taken literally from the Persons Database (BRP) or from the identification document submitted. However, it may be the case that the name details contain special characters which are not part of the standard character set in accordance with ISO8859-1 (Latin-1)[7]. If the name contains characters which are not part of this character set, the UZI register will carry out a transition. If names are longer than permitted in the certificates, the UZI register will use the hyphenation rules in accordance with 'NEN 1888:2002 (nl), General personal details; Definitions, character sets and exchange formats' of the NEN. This means that the last position of a field is replaced by a hyphen.

7 The character set used by the UZI register has the largest number of diacritic characters. This set does not include special characters, for example a Y with a diaeresis.

The UZI register reserves the right to change the requested name upon registration if this is legally or technically necessary.

3.1.5 Uniqueness of names

The UZI register guarantees that the uniqueness of the 'subject' field will be maintained. This means that the distinctive name which is used in an issued certificate can never be allocated to another subject. This is done by using the UZI number that is included in the subject.serialNumber (see chapter 7 for a more detailed explanation).

For the 'care provider' [zorgverlener] and the 'named employee' [medewerker op naam] cards, the UZI number is uniquely linked to the natural person. Any new card application for the same natural person, will contain the same UZI number. If a 'care provider' [zorgverlener] or 'named employee' [medewerker op naam] applies for cards for various institutions, these cards will contain the same UZI number. A person will only be issued a new UZI number if the birth name including prefixes and/or first names change. In the card for an 'unnamed employee' [medewerker niet op naam] and in server certificates, the UZI number is linked to the UZI card. A new UZI number is generated each time a new card application is submitted. The UZI register generates the UZI number from the same series of numbers for all types of card.

In instances in which parties are unable to agree on the use of names, the TSP management will decide after weighing up the interests involved, insofar as this is not provided for in mandatory Dutch law or other applicable regulations.

3.1.6 Recognition, authentication and role of trademarks

The name of an organisational association as referred to in the excerpt of a recognised register, a document of establishment, a notarial deed, an institution decision, a licence or in the law, will be used during registration and in the certificates.
The certificate managers bear full responsibility for any legal consequences of using the name they provide. In the event that brand names are used, the UZI register will take the necessary care, but is not obliged to initiate an investigation into possible violations of trademarks as a consequence of using a name which is part of the details included in the certificate. The UZI register reserves the right to change the requested name if it could be contrary to trademark law.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The key pairs are generated in a cryptographic module, in a controlled and protected environment, as part of the personalisation procedure, and then incorporated into the smart card via a secure communication session. The personal key cannot be removed from the smart card.

The key pairs for server certificates are not generated centrally, but by the subscriber's certificate manager. An application for certification of a public key of a server certificate is signed with the corresponding private key. In this way the certificate manager can demonstrate ownership of the private key.

3.2.2 Authentication of organization identity

If an organisation submits an application to be registered as subscriber in the UZI register, the following must be considered:

- A completed application form signed by the legal representative of the registration containing:
  - the full name of the organisation;

  - the address details of the organisation;
  - the full name (full first names, prefixes birth name, birth name, prefixes surname and surname) and contact details of the legal representative of the organisational identity.
  - the full name and contact details of the authorised applicant/applicants that may apply for and withdraw UZI cards on behalf of the organisation.
  - (optional) the AGB code (care institution code or practice code).
- Proof that the name of the organisational identity is up-to-date and correct. This proof can take the form of:
  - the registration number under which the organisational identity is listed in the Trade Register of the Chamber of Commerce and which shows the accuracy of the name;
- Proof that the legal representative is authorised to represent the organisation. This proof can take the form of:
  - the registration number under which the organisational identity is listed in the Trade Register of the Chamber of Commerce and which shows the authority;
  - copy of the document appointing the legal representative. Only when the legal representative does not appear from the Commercial Register of the Chamber of Commerce.
- Proof that the names of the people referred to in the application form are correct. This proof must be submitted in the form of a copy of an identification document as referred to in the Compulsory Identification Act [Wet op de Identificatieplicht] (WID). All first names must be written out in full on the submitted identification document. The identification document submitted must be valid on the date of registration. The UZI register archives the copies of the submitted identification documents.
- Proof that the organisational identity belongs to the domain of the UZI register. Please refer to Annex 2 for a more detailed explanation. Organisations that provide care on the basis of a law adopted by the House of Representatives and the Senate, have an accreditation within the meaning of the Care Institutions (Accreditation) Act [Wet toetreding zorgaanbieders] (Wtza) or are included in the Pharmacies Register within the framework of the Medicines Act [Geneesmiddelenwet] belong to the domain and do not need to submit any additional proof. If the organisation does not fall under these categories, proof must be submitted in the form of:
  - a copy of a document of establishment or notarial deed;
  - a copy of a licence or decision;
  - a care agreement;
  - a signed personal statement by all parties involved (only to be submitted if the organisation does not have legal personality).
- Data from subscriber organizations registered with the UZI-register are shared with the National Service for Identity Data (RvIG) for inclusion on the BSN authorization list[8].
- If applicable, the subscriber can indicate on the application form that his data[9] may be shared once with VZVZ. In the absence of this permission, no data will be shared with this organization.

The UZI register checks the authenticity, completeness and accuracy of the submitted documents. The UZI register checks whether any AGB code submitted corresponds to the AGB code in the Vektis registration. The UZI register checks whether the organisation belongs to the domain of the UZI register (see Annex 2). If

8 https://www.rvig.nl/bsn/autorisatielijst-bsn-gerechtigden. Shared data includes Subscriber number, subscriber name and date of registration UZI-register.

9 Subscriber number, subscriber name, profession and specialism or category of healthcare institution, visitingaddress, postal address, telephone number, e-mail address, agb code, Chamber of Commerce number, registration date, personal data of legal representative and authorized applicant.

proof of this is submitted in the form of a personal statement, the UZI register will request the underlying evidence on a random basis before registration takes place. The UZI register informs the subscriber of the registration or rejection of the registration request. In the event of a rejection, the reason for the rejection will be stated.

3.2.3 Authentication of individual identity

The personal identity is authenticated upon registration as a subscriber and upon the issue of an UZI card.

Registration of a person as a subscriber

If a care provider working alone submits an application to be registered as a subscriber in the UZI register, the following must be submitted:

- A completed application form signed personally by the care provider containing:
  - the full name of the care provider (birth name, including prefixes and first names);
  - the contact details (email address and (mobile) telephone number) of the care provider;
  - the professional title or qualification title of the care provider and reference to the assessment criteria to be applied (see Annex 2);
  - (optional) the AGB code of the care provider;
  - the address details of the care provider.
- Proof that the name details of the person referred to in the application form are correct. This proof must be submitted in the form of a copy of an identification document as referred to in the WID. All first names must be written out in full on the submitted identification document.. The UZI register takes the first names, prefixes birth name, the birth name and the Citizen Service Number (BSN) from the identification document and will archive the copy of the identification document.
- Professionals as referred to in Article 34 of the Individual Healthcare Professions Act who are not registered with the Paramedics' Quality Register [Stichting Kwaliteitsregister Paramedici], the Oral Hygienists' Quality Register [Kwaliteitsregister Mondhygiënisten], the Pharmacy assistants Quality Register must submit, as proof that they are allowed to use the qualification title, an original and validly authenticated copy of the diploma in question, or a digital excerpt (PDF with certificate from DUO).
-

The UZI register checks the authenticity, completeness and accuracy of the submitted documents. The UZI register checks whether the applicant can be designated as a care provider (see Annex 2). The UZI register checks whether any submitted AGB code corresponds to the AGB code of the person in the Vektis registration. The UZI register informs the subscriber of the registration or rejection of the registration request. In the event of a rejection, the reason for the rejection will be stated.

Applying for and issuing the UZI products

An application for UZI products must be made by an applicant. This is the legal representative or an applicant who is financially authorised on behalf of the subscriber. The application takes place digitally via the application on the website of the UZI register (www.uziregister.nl/aanvragen) or by using a paper application form.

The UZI register offers the digital application facility for the following types of products:

- Care Provider card [zorgverlenerpas] Article 3 and 36A of the Individual Healthcare Professions Act (with the exception of the specialisms of

paediatrician [jeugdarts], dispensing GP [apotheekhoudend huisarts] and A&E doctor [SEH-arts])
- Named employee card [medewerkerpas op naam]
- Unnamed employee card [medewerkerpas niet op naam]
- Server Certificates

For the above-mentioned card types, the UZI register can issue a paper application form (pdf format) at the request of the card applicant.

For the care provider card types [zorgverlenerpas] Article 34 of the Individual Healthcare Professions Act and the exceptions referred to in conjunction with the care provider [zorgverlenerpas] card Article 3 of the Individual Healthcare Professions Act, the UZI register offers a paper application form via the website.

The UZI register offers the possibility to submit documents digitally via a secure upload page.

Access to the digital application facility on the website of the UZI-register
The digital application facility on the website of the UZI-register can be used by the legal representatives or financially authorised applicants with one or more active subscription registrations within the UZI register. The person provides proof of identity via DigiD or a personal UZI card. The UZI register then checks whether this person is registered as a legal representative or financially authorised applicant with one or more active subscribers. If this is the case, access will be granted to the digital application facility and one or more UZI products can be applied for.

The facility displays the following details of the subscriber: the name of the subscriber, the subscription number, the name and contact details of the applicant. If the applicant is authorised for various subscribers, the applicant first selects the desired subscriber.

Applications via the digital application facility on the website of the UZI-register
Automatic links with the Personal Records Database (BRP) and the BIG register are used. These links are used to validate details that have been filled in when the application was made or to retrieve details from the register in question.

An indication per type is given below as to which details are necessary for the digital application and which documents have to be submitted for the UZI card to be issued and providing the server certificate.

Named employee card [medewerkerpas op naam]
- Digital application via www.uziregister.nl/aanvragen
  - Citizen Service Number (BSN) and date of birth of the intended cardholder. These details are used as a basis for verification in the Personal Records Database (BRP) and the birth name is retrieved and displayed.
  - Statement by the card applicant that the intended cardholder has granted explicit permission to use his/her personal details for the UZI card application.
  - The contact details (email address and mobile telephone number) of the intended cardholder. These details are needed for the issue of the UZI card.
  - As regards delivery of the PIN letter, the card applicant chooses the postal address of the subscriber or the home address of the intended cardholder. The home address is taken from the Personal Records Database (BRP) and is not displayed for reasons of privacy.
  - Use of name in correspondence. The card applicant chooses the partner name registered in the Personal Records Database (BRP) or the birth name

of the intended cardholder referred to in the Personal Records Database (BRP).

- The card is issued personally to the intended cardholder, with the intended cardholder being required to submit a valid, legal identity document as referred to in the Compulsory Identification Act [Wet op de Identificatieplicht] (WID). The identity document submitted must contain all forenames in full. The UZI register is obliged to archive a copy of the document used to prove identity. The physical confirmation of the identity of the cardholder and the creation of the copy are carried out by AMP Groep courier company at the instruction of the UZI register.

Care Provider card [zorgverlenerpas] Article 3 of the Individual Healthcare Professions Act (with the exception of the specialisms of paediatrician, dispensing GP and A&E doctor)

Professionals as referred to in Article 3 of the Individual Healthcare Professions Act must be registered in the BIG register.

- Digital application via www.uziregister.nl/aanvragen
  - Citizen Service Number (BSN) and date of birth of the intended cardholder. These details are used as a basis for verification in the Personal Records Database (BRP) and the birth name is retrieved and displayed.
  - Statement by the card applicant that the intended cardholder has granted explicit permission to use his/her personal details for the UZI card application.
  - Individual Health Care Professions Act (BIG) registration The BIG register assessment is carried out on the basis of the filled-in BIG number and a set of previously obtained personal details. The professional title and any specialism(s) are retrieved and shown in accordance with the registration in the BIG register. The applicant selects the desired specialism (ór *No Specialism*) to be included on the Care Provider card.
    Note: A Care provider card can only contain one specialism. A specialism cannot be added to the card afterwards.
  - The contact details (email address and mobile telephone number) of the intended cardholder. These details are needed for the issue of the UZI card.
  - As regards delivery of the PIN letter, the card applicant chooses the postal address of the subscriber or the home address of the care provider. The home address is taken from the Personal Records Database (BRP) and is for reasons of privacy not displayed.
  - Use of name in correspondence. The card applicant chooses the partner name or the birth name of the intended cardholder, as registered in the Personal Records Database (BRP).
  - The card is issued personally to the intended cardholder and can be done at any address[10] in the Netherlands, with the intended cardholder being required to submit a valid, legal identity document as referred to in the Compulsory Identification Act [Wet op de Identificatieplicht] (WID). The identity document submitted must contain all forenames in full. The UZI register is obliged to archive a copy of the document used to prove identity. The physical confirmation of the identity of the cardholder and the creation of the copy are carried out by AMP Groep courier company at the instruction of the UZI register.

Unnamed employee card [medewerkerpas niet op naam]

- Digital application via www.uziregister.nl/aanvragen
  - Job name for which the card is applied. A choice is made from a fixed selection of job names. See section 3.1.4.
- The card is issued personally to the card applicant and can be done at any address[10]n the Netherlands, with the card applicant being required to submit a valid, legal identity document as referred to in the Compulsory Identification Act

10 Different service levels apply to the Waddeneilanden.

[Wet op de Identificatieplicht] (WID). The identity document submitted must contain all forenames in full. The UZI register is obliged to archive a copy of the document used to prove identity. The physical confirmation of the identity of the card applicant and the creation of the copy are carried out by AMP Groep courier company on the instruction of the UZI register.

Server certificate

- Digital application via www.uziregister.nl/aanvragen by the subscriber's applicant/certificate manager containing:
  - the name of the subscriber;
  - the subscriber number;
  - the name of the applicant/certificate manager;
- the contact details (email address and mobile telephone number) of the applicant;the fully qualified domain name (FQDN) owned by the subscriber or which the holder has given permission to use. The domain name must be unique and may not be in use by another organisation. If the subscriber is not the owner of the domain name, the UZI-register checks if the subscriber can use the domain name.The methods used by the UZI-register are described in section 3.2.2.4.2, 3.2.2.4.18 and 3.2.2.4.7 of the Baseline Requirements.
- The PKCS#10 file (Certificate Signing Request(CRS)). PKCS#10 is the general standard for a certificate application and contains the public key which is included in the UZI server certificate. The PKCS#10 file must be added to the application via an upload functionality in the application form.

An indication is given below per card type as to which details are necessary for the application and which documents have to be submitted for the UZI card to be issued.

Care Provider card [zorgverlenerpas] Article 34 of the Individual Healthcare Professions Act and Article 3 of the Individual Healthcare Professions Act for the specialisms of dispensing GP [apotheekhoudend huisarts] , paediatrician [jeugdarts] and A&E doctor [SEH-arts])

- A completed application form signed by the subscriber's card applicant containing:
  - the name of the subscriber;
  - the subscriber number;
  - the name of the card applicant;
  - the full name (birth name, including prefixes and first names) of the intended cardholder;
  - the contact details (email address and mobile telephone number) of the intended cardholder;
  - the professional title or qualification title and any specialism of the intended cardholder and the reference to the applicable assessment criteria;
- Proof that the name details of the intended cardholder are correct. This proof must be submitted in the form of a copy of an identification document as referred to in the WID. All first names must be written out in full on the submitted identification document. The UZI register takes the first names, prefixes birth name, the birth name and the Citizen Service Number (BSN) from the identification document and will archive the copy of the identification document.
- Professionals as referred to in Article 34 of the Individual Healthcare Professions Act must either be registered with the Paramedics' Quality Register [Kwaliteitsregister Paramedici], the Oral Hygienists' Quality Register [Kwaliteitsregister Mondhygiënisten], the Pharmacy assistants Quality Register [Kwaliteitsregister Apothekersassistenten] (KAA) or must submit, as proof that they are allowed to use the qualification title, an original, authenticated copy of the diploma in question, or a digital excerpt (pdf with certificate from DUO).

- Professionals as referred to in Article 3 of the Individual Healthcare Professions Act that wish to include the specialism of dispensing GP [apotheekhoudend huisarts] in the certificate, must be registered in the overview 'Valid APG licenses'.This overview is managed by pharmatec, https://www.farmatec.nl/.
- The card is issued personally to the intended cardholder and can be done at any address[11] in the Netherlands, with the intended cardholder being required to submit a valid, legal identity document as referred to in the Compulsory Identification Act [Wet op de Identificatieplicht] (WID). A driving licence is not acceptable. The UZI register is obliged to archive a copy of the document used to prove identity. The physical confirmation of the identity of the cardholder and the creation of the copy are carried out by AMP Groep courier company at the instruction of the UZI register.

In the case of a digital application, the UZI register verifies personal details in, and retrieves personal details from, the Personal Records Database (BRP). In the other cases the UZI register checks the authenticity, completeness and accuracy of the submitted documents. In the case of an UZI card application for a care provider the UZI register also checks whether the intended certificate holder can be designated as a care provider (see Annex 2). In the case of a server certificates application for a domain name, the UZI register checks with the recognised registers (Foundation for Internet Domain Registration in the Netherlands [Stichting Internet Domeinregistratie Nederland] (SIDN) or Internet Assigned Numbers Authority (IANA)) to determine whether the subscriber owns the domain name, or when it is not the owner if the subscriber has permission from the domain owner to use the domain name. The UZI register informs the subscriber of the issue of the card or the rejection of the card application. If the card application is rejected, the reason for the rejection will be stated.

3.2.4 Non-verified subscriber information

The UZI register verifies all details included in the certificate, with the following exceptions:

- the 'department' field in unnamed employee cards [medewerkerpassen niet op naam]
- the 'department' field in Server Certificates.

Details which are issued for correspondence purposes by the card applicant, such as correspondence name, email addresses and telephone numbers are not verified.

3.2.5 Validation of authority

The subscriber's legal representative can, upon registration, record which people are allowed to apply for certificates for the subscriber. These applicants are also certificate managers and are entitled to receive a certificate for a certificate holder on behalf of the subscriber. The UZI register checks the authenticity of this application by the legal representative.
Only a legal representative can indicate who may apply for cards on behalf of the subscriber. The method used to authenticate the legal representative is described in section 3.2.2. In the case of a digital application the UZI register checks, on the basis of the authentication via DigiD or the UZI card, whether the application has been made by an authorised card applicant. In the case of a paper application this is done on the basis of a copy of an identity document or the 'wet' signature on the application form.

3.2.6 Criteria for interoperation

No stipulation.

11 Different service levels apply to the Waddeneilanden.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The procedures and checks relating to identification and authentication in the event of renewal of the certificate are the same as those which apply to initial registration. A new key pair is always generated when a renewal request is executed. If applicable, a new smart card is issued.

The UZI register sends the subscriber a letter with information about renewing the certificate. This letter will be sent 70 days before the expiration date of the UZI card. UZI cards can be renewed on the UZI-register website. Data which is already known to the UZI register, including personal details and professions as referred to in the Individual Healthcare Professions Act, do not need to be resubmitted. The new certificate comes into effect at the moment at which the new UZI card is produced.

Please note: All types of UZI cards, with the exception of the specialisms referred to below, can be renewed on the UZI-register site. The UZI register can issue a paper application form (PDF format) at the request of the card applicant. In this form, details which are already known to the UZI register will not be preprinted.

For the Article 3 Individual Healthcare Professions Act professions of which the specialism, such as paediatrician [jeugdarts] and dispensing GP [apotheekhoudend huisarts], are not registered under the cardholder's BIG number, no renewal can be carried out via the digital application facility. A completed application form will be required, signed by the subscriber's card applicant.

An UZI server certificate can be renewed via Digital application www.uziregister.nl/aanvragen. The renewal of a UZI server certificate by the same applicant does not require identity determination
When renewing certificates, a check must always be carried out in advance to see whether all the requirements of sections 3.1 and 3.2 have been fulfilled.

3.3.2 Identification and authentication for re-key after revocation

The procedures and checks relating to renewing keys after revocation of the certificate are the same as those which apply to the initial registration. A new key pair is always generated when a renewal request is executed. If applicable, a new smart card is issued. See the procedure in section 3.3.1 'Identification and authentication for routine re-key'.

3.4 Identification and authentication for revocation requests

The cardholder/certificate holder or a card applicant/certificate manager can submit revocation requests on behalf of the subscriber. Revocation requests can be made electronically, by telephone, by email or by post. It is not possible to withdraw server certificates by telephone[12].

- In the case of electronic revocation, identification and authentication take place on the basis of smart card number and revocation code. The revocation code is made available to the certificate holder in writing when the card is issued.
- In the case of telephone revocation, identification and authentication take place on the basis of an assessment of the details present in the UZI register. The revocation applicant must at least be able to issue a number of predetermined

12 This decision followed after a risk analysis. The revocation of a server certificate can have consequences as regards connecting a subscriber to the care infrastructure. Because the possibility of a wrongful revocation is greater in the case of a telephone request than when other channels are used, the UZI register does not offer the option of withdrawing server certificates by telephone.

details about the cardholder and the card involved. It is not possible to withdraw server certificates by telephone.

- In the case of revocation by normal email, identification and authentication will take place on the basis of:
  - A revocation request signed by an authorised person.
  - Proof of the identity of the party submitting the revocation request. This proof must be submitted in the form of a copy of an identification document as referred to in the Compulsory Identification Act [Wet op de Identificatieplicht] (WID). The identification document must be valid on the date of the revocation request. The UZI register will archive a copy of the identification document.
- The following requirement applies in the case of revocation by electronically signed email:
  - The email is signed by the person authorised to withdraw with a qualified non-repudiation certificate (as on the UZI card for care providers and named employees or another PKI government card).
- The same requirements apply to a revocation by post as to a revocation by normal email.

The UZI register checks whether the party submitting the revocation request is authorised to submit the application. In the case of revocation requests by normal email or post, the UZI register also checks the identity of the party submitting the revocation request on the basis of the submitted identity document or a previously archived copy of the identity document.

4 Certificate Life-cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

Applications for certificates can only be submitted by registered applicants and Legal representative subscriber. These applicants must themselves be subscribers to the UZI register or must be authorised to submit applications by the legal representative of the subscriber. PKCS#10 files can only be sent via the website or via electronically signed mail.

4.1.2 Enrollment process and responsibilities

It is not possible for a care provider to obtain several active cards with the same basic profession or specialism via a subscription registration. When renewing certificates, it is permitted for both certificates to be active for a limited period in order to ensure continuity. This period is set at 70 days. Once the application has been registered, the RA will issue instructions to produce the UZI card. The CA generates and publishes the certificates. The UZI register informs the intended certificate holder that the UZI card can be delivered and where and how.

It is not possible to cancel an application after submission to the UZI register. Exceptions are, at the discretion of the TSP management. These include, for example, the situation in which the applicant discovers an irregularity in the application immediately after submission, and the application is not yet being processed by the UZI register.

4.2 Certificate application processing

Before certificates can be applied for, the care provider must be registered as a subscriber with the UZI register. The following steps have to be completed:

- The intended subscriber submits a completely filled in and signed application form, including the documents indicated in section 3.2. The intended subscriber can fill in forms on the website of the UZI register. The subscriber can find out about all the applicable conditions via the CPS.
- The UZI register carries out the checks referred to in section 3.2 and informs the subscriber of the result.

A subscriber to the UZI register can apply for certificates. The following steps have to be completed:

- As regards applying for a Care Provider card [zorgverlenerpas] Article 3 Individual Healthcare Professions Act *(with the exception of the specialisms of paediatrician, dispensing GP and A&E doctor)*, a named employee card [medewerkerpas op naam] and an unnamed employee card [medewerkerpas niet op naam], the card applicant logs in to the digital application facility on the website. The card applicant then chooses the desired card type and fills in the application form and submits it digitally.
- For the above-mentioned card types, the UZI register can issue a paper application form (PDF format) at the request of the card applicant.
- For the other UZI resources the card applicant submits a completed and signed application form, including the documents indicated in section 3.2.3. The applicant can obtain forms via the website of the UZI register.
- The card applicant and the intended cardholder can find out about all the relevant conditions via the CPS.

The UZI register archives the submitted documents so that they can be used as proof in the event of reconstruction.

For server certificates, the UZI register does not check any Certification Authority Authorization DNS details on behalf of any 'certificate pinning' by the subscriber.

4.2.1 Performing identification and authentication functions
The UZI register carries out the checks referred to in section 3.2 and section 4.3

4.2.2 Approval or rejection of certificate applications
The UZI register carries out the checks referred to in section 3.2 and informs the subscriber of the issue or rejection of the card application. If the card application is rejected, the reason for the rejection will be stated.

4.2.3 Time to process certificate applications
In the case of a digital application via the web application the turnaround time from the submission of the application up until the moment at which the UZI card is made available for delivery is no more than threeweeks. The maximum turnaround time required for the UZI register to process a complete and properly filled in paper application form is eight weeks. The UZI register may require more time during extremely busy periods.
Approval or rejection of certificate

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The issue method differs for the various types of card. The methods used by the UZI register are described below per card type.

Care Provider card [zorgverlenerpas] and named employee card [medewerkerpas op naam]
The card for the Care Provider and the named employee is issued as soon as the intended certificate holder appears.

- The intended cardholder must appear in person at the address indicated by the card applicant. The UZI card can only be issued within the Netherlands[13].
- The intended cardholder submits a valid identification document showing his/her full first name(s), birth name and date of birth. Valid identification documents are those designated as such in Article 1 of the Compulsory Identification Act [Wet op de Identificatieplicht] (WID). All first names must be written out in full on the submitted identification document. The UZI register is obliged to archive a copy of the document used to prove identity. The data on the copy that are not relevant to the UZI register are shielded using automatic recognition software. An extract from the civil register or a copy of the birth certificate can serve as additional proof of the full first names.
- The physical confirmation of the identity of the intended cardholder and the creation of the copy are carried out by AMP Groep courier company on the instruction of the UZI register. AMP Groep is fully certified to do this (in accordance with ETSI EN 319411-2). AMP Groep checks the validity and authenticity of the identity document submitted. On the basis of this document and the physical appearance of the intended cardholder, AMP Groep carries out

13 Different service levels apply to the Waddeneilanden.

the identity check and also checks whether the person is the person authorised to hand over the UZI card in question.
- In the event of a positive result for all checks, the intended cardholder signs the confirmation of receipt. AMP Groep checks the signature on the basis of the submitted identification document.
- After signing, the UZI card is handed over and the date and time of handing over are recorded. Both parties will receive proof of this.
- In the case of a negative result for one of the checks, the UZI card will not be issued.

If the card holder does not schedule an appointment for the delivery of the UZI card by AMP Groep, AMP Groep will send several reminders. If the final delivery date is exceeded, the UZI card will be disabled by AMP Groep and returned to CIBG and the certificates will automatically be revoked.

Unnamed employee card [medewerkerpas niet op naam]
The unnamed employee card [medewerkerpas niet op naam] is issued on the basis of indirect appearance. The certificate holder is represented by a certificate manager of the subscriber that submitted the application.
- The intended cardholder/certificate manager must appear in person at the address indicated by the card applicant. The UZI card can only be issued within the Netherlands[14].
- The cardholder/certificate manager submits a valid identification document stating full first name, initials or other first name(s) (if applicable), birth name, as well as the date and place of birth. Valid identification documents are those designated as such in Article 1 of the Compulsory Identification Act [Wet op de Identificatieplicht] (WID). The UZI register is obliged to archive a copy of the document used to prove identity. The data on the copy that are not relevant to the UZI register are shielded using automatic recognition software.
- The physical confirmation of the identity of the card applicant/certificate manager and the creation of the copy are carried out by AMP Groep courier company on the instruction of the UZI register. AMP Groep is fully certified to do this (in accordance with ETSI EN 319411-2). AMP Groep checks the validity and authenticity of the submitted identity document. On the basis of this document and the physical appearance of the card applicant/certificate manager, AMP Groep carries out the identity check and also checks whether the person is the person authorised to hand over the UZI card in question.
- In the case of a positive result for all checks, the card applicant/certificate manager signs the confirmation of receipt. The card holder hereby agrees to the terms and conditions as stated in this CPS, see 4.4. AMP Groep checks the signature on the basis of the submitted identification document.
- After signing, the UZI card is handed over and the date and time of handing over are recorded.
- In the case of a negative result for one of the checks, the UZI card will not be issued.
- If the card holder does not schedule an appointment for the delivery of the UZI card by AMP Groep, AMP Groep will send several reminders. If the final delivery date is exceeded, the UZI card will be disabled by AMP Groep and returned to CIBG and the certificates will automatically be revoked.

Server certificate
A Server Certificate can be issued in two ways. Both are clarified below.

The Server Certificates are issued on the basis of a request signed by the applicant/certificate manager with an electronic signature:

14 Different service levels apply to the Waddeneilanden.

- The applicant/certificate manager signs the PDF application form with a qualified non-repudiation certificate (as on the UZI card for care providers and named employees). Ór;
- The applicant/certificate manager sends the UZI register an email containing the completed application form. The applicant/certificate manager signs this email with a qualified non-repudiation certificate (as on the UZI card for care providers and named employees).
- The employee of the UZI register checks the submitted details and carries out validity checks on the electronic signature. After carrying out the checks and recording the details, instructions are issued to produce the server certificate.

The server certificates are issued after the applicant/certificate manager of the subscriber has appeared in person:

- Theapplicant/certificate manager must appear in person at the address indicated. This physical confirmation of the identity of the applicant/certificate manager can only be carried out within the Netherlands.
- The certificate manager submits a valid identification document stating full first name, initials or other first name(s) (if applicable), birth name, as well as the date and place of birth. Valid identification documents are those designated as such in Article 1 of the Compulsory Identification Act [Wet op de Identificatieplicht] (WID). The UZI register is obliged to archive a copy of the document used to prove identity. The data on the copy that are not relevant to the UZI register are shielded using automatic recognition software.
- The physical confirmation of the identity of the card applicant/certificate manager and the creation of the copy are carried out by AMP Groep courier company on the instruction of the UZI register. AMP Groep is fully certified to do this (in accordance with ETSI EN 319411-2).
- The applicant/certificate manager signs the proof of identification. The certificate manager hereby agrees to the terms and conditions as stated in this CPS, see 4.4. After successful identification, the applicant/certificate manager will receive a confirmation by e-mail from AMP group.
- After the signed proof of identification has been processed by the UZI register, instructions will be given to produce the server certificate.

  If the identity of the applicant/certificate manager has been established earlier by the UZI register, then there is no longer any need to make an appointment for identity determination for the application of a UZI server certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

- After a servercertificate has been produced, the UZI register sends the certificate by email to the applicant/certificate manager. The UZI register also sends a revocation code to the subscriber's correspondence address for the attention of the applicant/certificate manager.
- For UZI cards there is no further notification to the subscriber of certificate issuance, the subscriber has already been informed on the outcome of de certificate application, see section 4.2

4.4 Certificate acceptance

The conditions for the use of certificates from the UZI register are published in this CPS.

4.4.1 Conduct constituting certificate acceptance

UZI card
By signing the confirmation of receipt, the certificate holder confirms receipt of the card to the UZI register. The UZI register records the time of issuing in accordance

with the confirmation of receipt. By taking receipt of the card, the certificate holder indicates that he/she is conversant with, and agrees to, the rights and obligations as referred to in the CPS and agrees with the content of the certificate. See also section 9.1.10.
Server Certificate
The certificate manager should check the certificate content on correctness and completeness before using it. By using the certificate, the certificate manager declares that he has taken note of and agrees with the rights and obligations as stated in the CPS and that he agrees with the content of the certificate. See also section 9.1.10.

4.4.2 Publication of the certificate by the CA
The certificates are published in the directory service immediately after the certificate has been signed by the CA during the production process.
Subscriber and card holder/certificate manager agree to the publication of the public certificates and the information contained therein, see chapter 7 and section 2.4.

4.4.3 Notification of certificate issuance by the CA to other entities
No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

- The subscriber guarantees that all submitted details are correct and complete. This concerns the details relating to the subscriber registration, the certificate application and other details.
- The subscriber guarantees explicitly that the subscriber's certificate holders will use the certificates applied for within the field of application as described in section 1.4 of the CPS and that the certificate holders will use the right certificate for the right purpose. The subscriber and the certificate holder are obliged to stop using the certificates and the corresponding private keys if instructed to do so by the UZI register. The UZI register can issue such an instruction in the event that a CA key is compromised. The subscriber and the certificate holder are obliged to inform the UZI register immediately and then withdraw the UZI card if an irregularity occurs as indicated in section 4.9.1. This applies both to the circumstances observed or suspected by the subscriber, and the circumstances which the certificate holders within the organisation report to the subscriber themselves. If applicable the certificate holder must submit the revocation code to the subscriber at the latter's explicit request. The subscriber and the certificate holder are obliged to take suitable measures to prevent unauthorised use of the private keys. This means, as a minimum, that the UZI cards are protected against damage, loss and/or theft, are not loaned out to third parties and are generally protected in the same way as valuable personal property such as credit cards or passports. In addition, the subscriber will ensure that the certificate holders within the organisation always keep the PIN, PUK code and the revocation code separately from the UZI card.
- The subscriber confirms that the UZI register is entitled to withdraw the UZI resources if the subscriber violates the applicable conditions or if the CIBG establishes that the certificate is being used in conjunction with criminal activities, for example phishing attacks, fraud, or the distribution of malware.
- The subscriber and applicant of UZI resources confirms that the UZI register is entitled to issue personal data, such as name, address, email and telephone number to Cannock Outsourcing B.V. and AMP Groep.

Obligations in relation to server certificates

The following additional obligations apply if the subscriber applies for server certificates:

- The subscriber guarantees that all data supplied, and therefore the data included in the certificate, are correct and complete. This concerns the data related to the subscription registration, the certificate application and other data
- The subscriber is obliged to save the keys which belong to server certificates in a Secure User Device (SUD). The subscriber must secure the SUD in which the private keys are saved in a manner suitable for securing critical company resources. The subscriber can deviate from this if compensatory measures are taken in the field of physical access security, logical access security, logging, audit and functional separation in the environment of the system that contains the keys of the server certificates. The keys can also be protected using software. The compensating measures must be obsessive quality that it is practically impossible to steal or copy the keys without being noticed[15].
- The subscriber must ensure that the key material of the certificate holders within the subscriber's organisation are exclusively generated in a safe resource that complies with EAL 4+ or equivalent security criteria.
- The subscriber is obliged to keep the activation details, which are used to obtain access to the private key(s) of the certificate holders within the organisation, separately from the SUD.
- If the fully qualified domain name (FQDN) as referred to in a server certificate is identifiable and addressable via the internet, the subscriber guarantees that the server certificate is only placed on a server that is at least accessible using one of the FQDNs in this server certificate.

The above obligations for the subscriber or certificate holder will be recorded and, insofar as they can be designated as too unspecific, will be developed into UZI register guidelines and/or more detailed regulations. Insofar as the provisions relate to UZI cards for which a subscriber has applied on behalf of the certificate holder within the subscriber's organisation, the rights and obligations between the subscriber and the certificate holder will have to be mutually recorded in writing.

4.5.2 Relying party, public key and certificate usage

The obligations of the trusting party are applicable when trusting a certificate issued by the UZI register. The trusting party is obliged:

- to assess on a case-by-case basis whether it is justified to trust the certificate;
- to check the validity and authenticity of the hierarchy within which the certificate is issued, meaning the validity of certificates of the more superior CAs as well as of the master certificate of the State of the Netherlands;
- to verify that the CA certificate -which is used to validate the signature under a qualified certificate- is included in the EU Trusted List of Qualified Trust Service Providers (QTSP)[16]. This is only applicable in order to rely on a signature certificate as an EU qualified certificate;
- to verify the validity of the certificate by means of the most recently published Certificates Revocation List (CRL) or via the Online Certificate Status Protocol (OCSP);
- always to use the most recently published Certificates Revocation List (CRL) in the event of calamities and/or incidents whereby the Online Certificate Status Protocol (OCSP) is inaccessible;
- to take cognizance of all obligations regarding the use of the certificate as referred to in this CPS and the trusting party conditions, including explicitly all restrictions on the certificate's use;
- to take all other precautionary measures which can reasonably be taken by trusting parties;

15 The UZI register has the right to check the compensating measures
16 https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/NL/1

- to be aware that previous checks only authenticated the integrity of the details and the identity of the certificate holder and, therefore, did not constitute a judgement on the content of the details.

4.6 **Certificate renewal**

If, after the (threatened) expiry of the period of validity or after an application for revocation, a new UZI card is applied for, new key pairs and new certificates will be generated. The procedures, checks and method of working used in relation to the application, production and issuing are the same as the procedures, checks and method of working relating to the first issue.
Certificate holders' keys will not be reused after the end of the period of validity or after the corresponding certificates have been withdrawn. Renewing certificates will also mean renewal of the key pair.

4.6.1 Circumstance for certificate renewal
No stipulation.

4.6.2 Who may request renewal
No stipulation.

4.6.3 Processing certificate renewal requests
No stipulation.

4.6.4 Notification of new certificate issuance to subscriber
No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate
No stipulation.

4.6.6 Publication of the renewal certificate by the CA
No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities
No stipulation.

4.7 **Certificate re-key**

If, after the (threatened) expiry of the period of validity or after an application for revocation, a new UZI card is applied for, new key pairs and new certificates will be generated. The procedures, checks and method of working used in relation to the application, production and issuing are the same as the procedures, checks and method of working relating to the first issue.

4.7.1 Circumstance for certificate re-key
No stipulation.

4.7.2 Who may request certification of a new public key
No stipulation.

4.7.3 Processing certificate re-keying requests
No stipulation.

4.7.4 Notification of new certificate issuance to subscriber
No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate
No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA
No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities
No stipulation.

4.8 **Certificate modification**
If certificates have to be modified, the certificates will have to be withdrawn and new certificates with amended details applied for.

4.8.1 Circumstance for certificate modification
No stipulation.

4.8.2 Who may request certificate modification
No stipulation.

4.8.3 Processing certificate modification requests
No stipulation.

4.8.4 Notification of new certificate issuance to subscriber
No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate
No stipulation.

4.8.6 Publication of the modified certificate by the CA
No stipulation.

4.8.7 Notification of certificate issuance by the CA to other Entities
No stipulation.

4.9 **Certificate revocation and suspension**
Requests to withdraw certificates can be submitted as described below. The UZI register ensures that the date and time of revocation of certificates can be determined precisely. In the event of any doubt the time determined by the UZI register will apply as the moment of revocation. If a certificate is withdrawn, it cannot be declared valid again.

The UZI register does not permit the (temporary) suspension of certificates.

4.9.1 Circumstances for revocation
The certificate holder or the subscriber are obliged to submit a request for revocation to the UZI register and stop using the certificate, including the corresponding keys, in the following circumstances:

- Loss, theft or failure of the bearer of the certificate (UZI card).
- Observed or suspected misuse or compromise.
- Definitive blocking of the smart card (if an incorrect PUK code has been entered three times).
- Termination of the subscriber's existence.
- Termination of the relationship between the subscriber and certificate holder.
- Inaccuracies in, or changes to, the details shown on the certificates.
- Failure to fulfil the assessment criteria as described in Annex 2.
- System/server no longer in use at the care institution.
- Permission to use the domain name is withdrawn.

Revocation on the initiative of the UZI register will take place in the following circumstances:

- The certificates of a subscriber or certificate holder can be withdrawn if the subscriber or certificate holder does not fulfil the obligations in the CPS.
- The certificates of a subscriber are withdrawn if the subscriber in question no longer fulfils the assessment criteria in Annex 2.
- A care provider card [zorgverlenerpas] is withdrawn if the holder is no longer permitted to use the professional title, qualification title or the specialism included in the certificate. In this context the UZI register may apply a transition period of one month for 'dying out' specialisms. A further clarification is included in the Annex 2.
- A server certificate is withdrawn if the owner of the domain name reports to the UZI register that the permission to use the domain name has been withdrawn.
- A server certificate is withdrawn if it is not paid for by the set deadline[17].
- The certificates of an UZI card are withdrawn if the card has not been issued within the set deadline of 6 weeks.
- The certificates of an UZI card are withdrawn if it has not been paid for by the set deadline.
- The certificates of a subscriber or certificate holder are withdrawn if the UZI register observes inaccuracies in the details included in the certificate, for example in the event of a name change.
- The certificates of a subscriber or certificate holder are withdrawn if the private key belonging to the certificates, or the key of the TSP or PKI government has been compromised.
- The certificates of a subscriber or certificate holder are withdrawn if the technical content of the certificate implies an irresponsible risk for subscribers, trusting parties and third parties (for example browser parties).

The reasons for each revocation initiated by the UZI register are documented and archived.

4.9.2 Who can request revocation

A request to withdraw certificates may be submitted by:

- the certificate holder itself of the certificate manager;
- the legal representative or an authorised card applicant of the subscriber;
- the curator that acts if the subscriber or certificate holder itself is no longer authorised to perform legal actions with intended legal consequence;
- the UZI register.

A trusting party cannot make a revocation request but can report the suspicion of a circumstance which may cause the revocation of a certificate. The UZI register will investigate such a report and will, if necessary, withdraw the certificate.

4.9.3 Procedure for revocation request

Requests to withdraw certificates can be made by an appropriately authorised person of the subscriber, or by the certificate holder electronically, by telephone, by email, or by post. It is explicitly pointed out that, in the event that the revocation serves an urgent interest, the revocation should take place electronically via the website of the UZI register (www.zorgcsp.nl). This form of revocation is available twenty-four hours a day, seven days a week.

In the case of an **electronic** revocation the applicant fills in the smart card number of the card to be withdrawn and the corresponding revocation code on the website of the UZI register. If the revocation code and smart card number are correct, the card will be withdrawn. The applicant will be notified on the website. If the revocation code and smart card number are incorrect, notification will be given that

17 As stated in section 9.1.7, the deadline is set at six weeks after receipt of the reminder.

the revocation will not be carried out. The UZI register has taken measures to make it impossible to make unlimited (incorrect) revocation requests.

In the case of a **telephone**[18] revocation, no documents are submitted. The party submitting the revocation request must answer a number of predetermined questions. Based on these questions, the UZI register must obtain sufficient certainty about the identity of the revocation applicant and the card for which the revocation application is being submitted. After establishing the identity of the party submitting the revocation request and of the card, the UZI register checks whether the party submitting is authorised to make the revocation application. After performing the checks, the UZI register will withdraw the certificates. A confirmation that the revocation has been taken care of, or a notification that the revocation request has been rejected will be sent in writing to the certificate holder.

In the case of revocation **by not-electronically signed email, or by post** the following types of proof must be submitted:

- A revocation request signed by an appropriately authorised person, containing:
  - the name of the subscriber;
  - the name of the person making the revocation request;
  - the reference to the card or cards to which the request applies.

The UZI register checks whether the signature on the revocation request corresponds to the archived copy of an identification document as referred to in the WID.

- If the signature corresponds, the UZI register will carry out the revocation request.
- If the signature does not correspond, the UZI register will telephone the subscriber using the contact details registered with the UZI register. The applicant will then be requested to place the signature in accordance with the WID archived with the UZI register. If the signature on the WID is changed, the applicant will be asked to send a valid copy of the WID to the UZI register. After another check of the signature, the UZI register will carry out the revocation request. The UZI register archives the new copy of the WID.
- If no identification document is known to the UZI-register, it must be enclosed with the application.

The following requirement applies in the case of revocation by **electronically signed email**:

- The email is signed by the person authorised to withdraw with a qualified non-repudiation certificate (as on the UZI card for care providers and named employees or another PKI government card).

The UZI register checks whether the party submitting the revocation request is authorised to submit the application. The UZI register also checks the identity of the party submitting the revocation request on the basis of the submitted identity document or a previously archived copy of the identity document. After carrying out the checks the UZI register withdraws the certificates and then places them on the Certificate Revocation List (CRL). A confirmation that the revocation has been taken care of, or a notification that the revocation request has been rejected will be sent in writing to the certificate holder.

4.9.4 Revocation request grace period

The certificate holder or the subscriber are obliged to submit a revocation request immediately and without delay to the UZI register in situations referred to in section 4.9.1.

18 As stated in section 3.4 it is not possible to withdraw server certificates by telephone.

4.9.5 Time within which CA must process the revocation request

Electronic requests are dealt with immediately online. The UZI register advises parties to use the electronic revocation facilities on the website of the UZI register. These facilities are available twenty-four hours a day and seven days per week. In the event of electronic and telephone revocation, the maximum delay between receiving a request and changing the revocation status information (CRL) is four hours.

Requests received by e-mail or post will only be processed within four hours if the request is received on workdays between 7:30 a.m. and 4:00 p.m. Requests submitted after 4:00 p.m. will be processed the following working day.
If the revocation has an urgent interest, this must be done electronically (24 hours a day and seven days a week using the revocation code) or by telephone (only possible on workdays between 9:00 a.m. and 5:00 p.m.).

4.9.6 Revocation checking requirement for relying parties

Trusting parties are obliged to check the current status (withdrawn/not withdrawn) of a certificate by consulting the most recently published CRL or via the OCSP facility. Trusting parties are also obliged to check the CRL's electronic signature, including the corresponding certification path.

4.9.7 CRL issuance frequency

The CRL issue frequency is every hour. In the event of system defects, service activities or other factors outside the control of the UZI register, the UZI register also ensures that revocation requests which are submitted via the registration website are carried out within four hours after submission. With this in mind a fallback scenario has been designed which is regularly tested.

If the processes which rely on the UZI certificates require the certificate status to be more up-to-date, we urgently advise using the facility for an online check of the revocation status (see section 4.9.9).

Revoked certificates remain on the CRL even after the original validity date has passed.

4.9.8 Maximum latency for CRLs

The CRL is published immediately after generation.

4.9.9 Online revocation/status checking availability

In addition to the publication of CRLs, the UZI register also offers certificate status information via the Online Certificate Status Protocol (OCSP) facility. The OCSP is structured in accordance with IETF RFC 6960. As soon as a CA certificate reaches the expiry date, the OCSP service stops for the CA in question.

OCSP validation is an online validation method whereby the UZI register sends the trusting party an electronically signed message (OCSP response) after the trusting party has sent a specific request for status information (OCSP request) to the OCSP service (OCSP responder) of the UZI register. The OCSP response will include the requested status of the certificate in question. The status can be expressed as one of the following values: good, withdrawn or unknown. If an OCSP response is not forthcoming for whatever reason, no conclusion can be drawn in relation to the certificate's status. The URL of the OCSP responder with which the revocation status of a certificate can be validated is stated in the AuthorityInfoAccess.uniformResourceIndicator attribute of the certificate.

An OCSP response is always sent and signed by the OCSP responder. A trusting party must verify the signature under the OCSP response with the system certificate

which accompanies the OCSP response. This system certificate is issued by the same Certification Authority (CA) as the CA that has issued the certificate of which the status is being requested.

The information issued via the OCSP responder may be more up-to-date than the information communicated via the CRL. This is only the case if a revocation has taken place and the regular renewal of the CRL has not yet occurred.

4.9.10 Online revocation checking requirements
This service is freely available to all trusting parties who want to validate the revocation status of a certificate issued by the UZI register.

4.9.11 Other forms of revocation advertisements available
No stipulation.

4.9.12 Special requirements re key compromise

Revocation of a domain or a TSP certificate will be considered if the signing key belonging to the certificate is compromised or suspected to be compromised. Indicators of private key compromise may include:

- Theft or loss of device holding a private key;
- Audit findings indicating private key compromise;
- CT Log findings indicating unauthorized certificate signing;
- Incidents reported to CIBG by third parties which may indicate key compromise.

All indicators are registered, analyzed, and followed up accordingly.

4.9.13 Circumstances for suspension
The UZI register does not permit the (temporary) suspension of certificates.

4.9.14 Who can request suspension
The UZI register does not permit the (temporary) suspension of certificates.

4.9.15 Procedure for suspension request
The UZI register does not permit the (temporary) suspension of certificates.

4.9.16 Limits on suspension period
The UZI register does not permit the (temporary) suspension of certificates.

4.10 Certificate status service

4.10.1 Operational characteristics
The UZI register issues a new CRL every hour. OCSP can be used to request the current status information.

4.10.2 Service availability
In the event of a disruption, the UZI register will ensure that the services become available again within four hours of the disruption being discovered. This only applies to the CRL. In the event of disruptions the CRL must always be used and not the OCSP.

4.10.3 Optional features
No stipulation.

4.11 End of subscription

Subscriber registration has no end date. If the relationship between the subscriber and the UZI register is terminated, the subscriber will be deleted from the UZI register.

With a request to delete the registration the subscriber indicates that he no longer wishes to use the services of the UZI register. The subscriber is then removed from the UZI register. A request for deletion of a subscriber's registration (and therefore revocation of the certificates issued to the subscriber) must be submitted in writing to the UZI register. The UZI register authenticates the applicant in accordance with the authentication procedure which applies to the registration applications.

4.11.1 Transition period for a care provider subscriber [zorgverlener abonnee]

A transition period of three months will come into effect in the event of the death, unconditional suspension or deletion from the BIG register of a care provider [zorgverlener] who is also a subscriber. This transition period implies the following:

- all named cards (care provider card [zorgverlenerpas] and named employee cards [medewerkerpassen op naam]) will be withdrawn in accordance with the applicable rules. This also applies to named cards which have been applied for and/or issued just before or during the transition period.
- Server Certificates will continue to be active.
- the subscriber registration will remain active.
- no new products may be applied for.

After the transition period, Server Certificates will be withdrawn and the subscriber registration deleted. If under the subscriber registration none or only UZI cards by name (the healthcare provider card and employee card by name) are active, the subscriber registration is immediately withdrawn.The UZI register does not provide any refund for the remaining period of validity of withdrawn UZI certificates.

4.11.2 Transition period for an organisation subscriber

A transition period of three months will come into effect in the event of a name change or termination of an institution that is a subscriber. This transition period implies the following:

- All personalised cards (care provider cards [zorgverlenerpassen] and named employee cards [medewerkerpassen op naam]), and also unnamed employee cards [medewerkerpassen niet op naam] and Server Certificates will remain active.
- the subscriber registration will remain active.
- no new products may be applied for.

After the transition period, all cards and Server Certificates will be withdrawn and the subscriber registration will be deleted. The UZI register does not provide any refund for the remaining period of validity of withdrawn UZI certificates.

4.12 Key escrow and recovery

The UZI register does not support key escrow and key recovery.

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 Facility, management, and operational controls

5.1 **Physical controls**

5.1.1 Site location and construction

The services of the UZI register are provided from various locations. The registration work is carried out at the CIBG's premises. The personalisation work takes place at the premises of the supplier of the personalisation services. The certification takes place at the computing centre of the CA services supplier. The work in relation to the mobile identification and issuance takes place on location.

5.1.2 Physical access

The necessary physical security measures have been taken for all locations. These measures have been taken on the basis of risk analyses and security plans. The measures taken guarantee a secure and properly protected registration, personalisation, certification, issuance and revocation process that prevents unauthorised access to, or violation of, these processes or the locations where they are being carried out. For example, the work relating to the certification takes place in a high security environment at a computing centre. This environment complies with legal regulations imposed by the government. Numerous measures have been taken at all locations to prevent emergency situations and to limit any emergency-related damage. Examples of these measures are lightning conductors, power supplies, structural measures and access procedures.

The UZI register has separate test, acceptance and production systems. The transfer of software from one environment to the other takes place in a controlled fashion via a change management procedure. This change management procedure covers, among other things, monitoring and recording versions, changes and emergency repairs to all operational software. Before software can be put into production, the UZI register carries out tests on the basis of predetermined test plans.

The UZI register takes prompt and coordinated action to respond quickly to incidents and to limit the effect of any security violation. All relevant incidents are immediately reported to the organisations stipulated in the law and regulations whenever they occur. Incidents relating to a category specified in advance by the Policy Authority of the PKI for the government are reported to said Policy Authority.

5.1.3 Power and air conditioning

See section 5.1.2

5.1.4 Water exposures

See section 5.1.2

5.1.5 Fire prevention and protection

See section 5.1.2

5.1.6 Media storage

All used system storage media are treated safely in order to protect them from damage, theft and unauthorised access. Storage media are carefully removed when they are no longer needed.

Usage capacity is monitored and predictions are made in order to ensure sufficient processing capability and storage capacity in the future.

5.1.7 Waste disposal
CIBG personnel are obliged to dispose of confidential information in the designated closed waste bins or shredders. A data destruction company has been contracted for the destruction of this confidential data.

5.1.8 Off-site backup
CIBG has taken measures to guarantee the availability of business-critical services. These measures, as well as the *Recovery Point Objective* and *Recovery Time Objective*, are described in a business continuity plan.

Incremental backups of the registration system and digital records are stored on a daily basis, full backups are stored on a weekly basis and are also archived at a remote location. The paper archive is not backed up.

5.2 Procedural controls

5.2.1 Trusted roles
Personnel with access to cryptographic material or people who also operate in a confidential role have a position that is classified as confidential. Hereby, all staff in confidential positions have been screened for the presence of conflicting interests that could influence the impartiality of the activities of the UZI-register. This by means of a 'Declaration on behaviour' in accordance with the Judicial Data Act.

5.2.2 Number of persons required per task
The services of the UZI register are organised in such a way that it is impossible for a single person to compromise the reliability of the services. Registration, personalisation, certification and issuance are organisationally separated tasks. The 'four eyes principle' and/or functional separation is applied to registration tasks.

5.2.3 Identification and authentication for each role
No stipulation.

5.2.4 Roles requiring separation of duties
The UZI register maintains functional separation of the implementation, decision-making and verification tasks. In addition, there is functional separation between system management and operation of the TSP systems, as well as between Security Officer(s), TSP Manager(s), System auditor(s), system administrator(s) and TSP operator(s).

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements
All employees involved in the services of the UZI register have extensive knowledge and experience in the field of certification services. All employees responsible for checking identification documents have the necessary knowledge to check the authenticity of the documents.

Security tasks and responsibilities, including confidential positions, are documented in the appropriate job descriptions. These have been drawn up on the basis of the separation of tasks and authorities and a specification of the sensitivity of the position.

Any employee authorisation is carried out on the basis of a 'need-to-know' principle. Procedures have been drawn up and implemented for all confidential and administrative tasks which affect the provision of certification services.

5.3.2 Background check procedures
Background checks are carried out on all employees involved in personalisation and certification work. The UZI register requests all employees involved in registration and issuance to provide a certificate of good conduct.

All employees who carry out tasks for the UZI register are able to take part in training and awareness activities which are relevant for the execution of their task.

5.3.3 Training requirements
The UZI register deploys sufficient personnel who have enough specialist knowledge, experience and qualifications which are necessary for the TSP services. Managers are fully aware of the nature of the certification services and corresponding quality level.

5.3.4 Retraining frequency and requirements
Specific training is obligatory for all personnel. An annually updated training plan is used to monitor training.

5.3.5 Job rotation frequency and sequence
No stipulation.

5.3.6 Sanctions for unauthorized actions
Any employee who performs an unauthorised action is immediately denied access to all systems. The TSP management decides on the duration and the conditions of the access denial and any additional actions and sanctions to be taken.

5.3.7 Independent contractor requirements
The aforementioned requirements apply to hired personnel. Personnel are hired on the basis of master contracts.

5.3.8 Documentation supplied to personnel
UZI register employees will be demonstrably provided with the documentation which is necessary for the proper fulfilment of the task assigned to them.

5.4 Audit logging procedures

5.4.1 Types of events recorded
The UZI register maintains overviews of:

- Creating accounts.
- Installation of new software or software updates.
- Date and time and other descriptive information concerning backups.
- Date and time of all hardware changes.
- Date and time of audit log dumps.
- Shutting down and (re)starting of systems.
- All registration activities relating to the application and revocation of certificates and any changes to registration details.

The UZI register manually or automatically monitors the following events:
- Life cycle events relating to the CA key, including:
  - generating keys, backup, storage, recovery, archiving and destruction;
  - life cycle events relating to the cryptographic equipment.
- Life cycle events relating to the management of certificates, including:
  - certificate applications, reissue and revocation;
  - successful or unsuccessful processing of applications;
  - generating and issuing certificates and CRLs.
- Security incidents, including:
  - successful and unsuccessful attempts to gain access to the system;
  - PKI and security activities undertaken by personnel;
  - reading, writing or deleting security-sensitive files or records;
  - changes to the security profile;
  - system crashes, hardware failure, and other irregularities.

The parts of the loggings contain the following elements:
- Date and time.
- Serial number.
- Author identity.
- Type.

5.4.2 Frequency of processing log
Loggings are investigated on a random basis and as part of internal quality processes.

5.4.3 Retention period for audit log
The consolidated loggings relating to life cycle management certificates are kept for a period of at least seven years and then deleted. The log files related to technical threats and risks are kept for 24 months and then deleted.

5.4.4 Protection of audit log
Events which are included electronically and manually in audit log files are protected against unauthorised perusal, change, deletion or other undesirable changes by means of physical and logical access control resources.

5.4.5 Audit log backup procedures
A backup of the audit log files is created daily and stored on an external location

5.4.6 Audit collection system (internal vs. external)
All audit logs are saved internally on the systems. In addition, logging is archived off-site. The most important log details are also archived each quarter at the CIBG.

5.4.7 Notification to event-causing subject
The UZI register carries out a more detailed investigation if the logging reveals malicious activities.

5.4.8 Vulnerability assessments
At least once a year the UZI register carries out a risk analysis, which includes a vulnerability analysis. On the basis of the outcomes of these analyses the UZI register implements suitable measures as necessary.

5.5 Records archival

5.5.1 Types of records archived
The UZI register archives all relevant information relating to events, details, files and forms. At least the following is recorded:
- Applications for registration and applications for certification (application forms).

- Documents submitted during the application procedure (including a copy of the identity document, excerpt from the Trade Register of the Chamber of Commerce, document of establishment and original, certified copy of a diploma).
- Storage location of copies of applications and identity documents.
- Information which is relevant for the identification of a subscriber or certificate holder.
- Information concerning the checks carried out.
- Correspondence relating to registration application or card application.
- Proof of date and time of issue of the certificates.
- Information concerning revocation requests of certificates or deletion from the registration.
- Complaints and correspondence received in relation to complaints.
- Information requests received in writing.

5.5.2 Retention period for archive
All archived events are stored in accordance with section 10.4 of the selection list[19] throughout the period of validity of the qualified certificate and for a period of seven years after the date on which the validity of the qualified certificate expires.

Alle archived events with regard to the subscription registration are stored for a period seven years from the date on which the subscription registration is deleted.

5.5.3 Protection of archive
The UZI register ensures the integrity and accessibility of the archived details. The UZI register arranges careful and secure storage and archiving.

5.5.4 Archive backup procedures
Incremental backups of the registration system and of digital documents are created on a daily basis. Full backups are carried out on a weekly basis and are also archived at an external location. No backup is made of the paper archive.

5.5.5 Requirements for time-stamping of records
All information on paper is accompanied by a date and/or a date of receipt.

Electronically stored information is accompanied by an indication of the date and time from the processing system used to perform the action. The processing systems are synchronised in accordance with the Network Time Protocol using a reliable time source based on the atomic clock in Frankfurt.

The date and time a card is issued is recorded upon issue and signed by both parties.

5.5.6 Archive collection system (internal or external)
Electronic archiving takes place at physically separated locations (online details synchronisation). Paper dossiers are stored at a single physical location.

5.5.7 Procedures to obtain and verify archive information
No stipulation.

5.6 **Key changeover**
If the CA starts using a new key pair, the new CA certificates will be added to the UZI card. In addition, the CA certificates will be made available in the directory and on the website.

19 Generieke Selectielijst voor de archiefbescheiden van het CIBG Dienst voor registers vanaf 1995- vallend onder het zorgdragerschap van het Ministerie van Volksgezondheid, Welzijn en Sport en Stichting Donorgegevens Kunstmatige Bevruchting vanaf 1995.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The UZI register has drawn up a calamities plan to minimise the consequences of any calamity that might occur. The Business Continuity Plan describes procedures and methods relating to fallback services.

In the event of any compromising of keys, or in the event of calamities, the UZI register may instigate an investigation, but this is not mandatory. In the event of a compromise of (one of) the private key(s) of the UZI register, the UZI register will undertake the following actions as a minimum:

- The UZI register will inform trusting parties, subscribers and certificate holders as soon as possible by publishing the information on www.uziregister.nl
- The UZI register will inform the subscribers in question via an email sent to the email address provided during registration.
- If necessary, the UZI register will immediately withdraw the certificates in question and publish them on the applicable CRL.
- The UZI register will immediately inform the PKI Policy Authority for the government, Radio communications Agency Netherlands 9 (AT), certifying authority and optionally Dutch Data Protection Authority (AP) in the event of a calamity.

In the event of a compromise of one of the algorithms used by the UZI register, the UZI register will consult with the PKI Policy Authority for the government. In principle the UZI register will follow the Policy Authority's guidelines. Before proceeding with large-scale revocation as a consequence of a compromise of an algorithm, coordination will take place with the Ministry of Health, Welfare and Sport.

5.7.2 Computing resources, software, and/or data are corrupted

See section 5.7.1.

5.7.3 Identity private key compromise procedures

See section 5.7.1.

5.7.4 Business continuity capabilities after a disaster

See section 5.7.1.

5.8 CA or RA termination

In the event that the UZI register terminates the certification services, this will be done in accordance with a controlled process described in more detail in the UZI register CA Termination Plan. This termination can be voluntary or involuntary in nature and this will determine the activities to be carried out.

Elements of the plan in the event of termination include:

- Communication with subscribers, trusting parties and other TSPs with which relationships exist or other forms of regular cooperation;
- Decommissioning of the relevant private CA keys;
- The publication service must continue to be active at least six months after termination;
- KPN B.V. will be instructed to perform the destruction of the CA keys on a date yet to be determined. KPN B.V. will submit an official document to the CIBG as proof of the destruction.
- Doc-Direkt will be instructed to destroy the dossiers. In accordance with Doc-Direkt PDC (see Central Government Portal).

6 Technical security Controls

6.1 Key pair generation and installation

When generating key pairs, the UZI register will use secure resources and reliable systems. The UZI register ensures that the reliability and the security of the systems fulfils internationally recognised standards and national legislation.

The keys are generated using equipment which complies with Common Criteria EAL 4+ or higher in accordance with ISO 15408 ('Cryptographic module for TSP Signing Operations') or equivalent security standard.

6.1.1 Key pair generation

When generating key pairs, the UZI register uses reliable procedures in a secure environment which complies with objective and internationally recognised standards.

The keys of the CAs of the UZI register were generated in a FIPS 140-2 level 3 certified Hardware Security Module (HSM). The keys of the CAs are 4096 bits RSA The keys of the (intended) certificate holders are generated in a FIPS 140-2 level 3 certified HSM. This involves the use of the signature algorithm 'sha256WithRSAEncryption'. The keys are injected via a secured communications channel in the smart card (Qualified Signature Creating Device - QSCD).

6.1.2 Private key delivery to subscriber

The UZI card (smart card with keys and certificates) is:

- Handed over in person to the certificate holder in the case of a 'care provider' [zorgverlener] or an 'named employee' [medewerker op naam]. The PIN, PUK code and revocation code are sent separately to the intended certificate holder in the form of a PIN letter.
- Handed over in person to the applicant/certificate manager on behalf of the subscriber in the case of an 'unnamed employee' [medewerker niet op naam]. The PIN, PUK code and revocation code are sent to the applicant separately in the form of a PIN letters.

The private key is not transferred in the case of server certificates. The certificate and the certified public key are sent to an email address provided during application once the applicant/certificate manager on behalf of the subscriber has appeared in person.

CIBG and its supplier monitor the QSCD certification status until the end of the validity period of the certificate and take appropriate measures in case of change in this status due to, for example, the expiry of the certification validity period or premature revocation of this certification. As a first step, the TSP management will be informed about this change in status and will, based on the situation encountered, implement further measures if necessary.

6.1.3 Transfer of the public key from the TSP to end users

The public key of the UZI register CA's, is signed by the PKI Government Domain CA, as a result of which the integrity and origin of the public key is safeguarded. The public keys of the underlying CAs are signed by the TSP CA. These public keys are made available by the UZI register to trusting parties, in the form of CA certificates, via www.zorgcsp.nl

A UZI card (smart card) is supplied with the full certificate hierarchy for the user certificate in question. CA certificates of the TSP are available via: https://cert.pkioverheid.nl/.

6.1.4 CA public key delivery to relying parties
The key pairs for UZI cards are generated by the personalisator. The public keys are sent via secured connections in signed messages to the CA for signing.

In the case of server certificates, the key pair is generated by the subscriber/applicant. In such instances the public key is also sent to the CA in a signed message via a secured connection.

6.1.5 Key sizes
The key length of a Certificate is at least 2048 bits RSA. The key length of a CA-Certificate is 4096 bits RSA.

6.1.6 Public key parameters generation and quality checking
The UZI register generates keys in smart cards or HSMs which comply with the FIPS 140-2 level 3 standard.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)
The certificates, including the corresponding key pairs, are exclusively intended for the purposes described in this CPS. The purposes for which a key may be used are included in the certificate (field: KeyUsage).

6.2 Private key protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls
For operational use, the cryptographic details are stored in a Hardware Security Module (HSM). The HSM fulfils the requirements described in FIPS 140-2 level 3 or higher.

6.2.2 Private key (n out of m) multi-person control
The private keys of the CAs of the UZI register cannot be read as a single entity.

A backup is made of the private keys of the CAs of the UZI register. The backup is saved in cryptographic modules in several encrypted parts. The backup can only be used if several parties are present with their part of the key.

6.2.3 Private Key Escrow
Since 1 October 2013 the UZI register has not supported key escrow and key recovery. This termination applies to all cards that were issued before that date.

6.2.4 Private Key backup
The UZI register does not make a backup of the private keys of certificate holders.

6.2.5 Private Key Archival
Private keys are never archived. Technical and organisational measures have been taken to ensure that it is impossible to archive these keys.

6.2.6 Private Key transfer into or from acryptographic module
In the case of private keys saved in a cryptographic hardware module, access security is used which ensures that the keys cannot be used outside the module.

6.2.7 Private key storage on cryptographic module
Private keys are saved securely throughout the entire lifespan.

6.2.8 Method of activating private keys

The private keys of the CAs of the UZI register can only be activated by means of a key ceremony and in the presence of the necessary officials. The UZI register ensures a careful procedure in a secured environment.

An activation code is issued for the activation of end users' private keys (see section 6.4).

6.2.9 Method of deactivating private keys

In certain circumstances, to be determined by the UZI register, the private keys will be deactivated with due regard for the applicable due diligence procedures.

If an UZI card that has been lost by the certificate holder is returned to the UZI register, the UZI register will destroy the card and the associated private keys. Any still active certificates belonging to the card will be withdrawn.

6.2.10 Method of destroying private keys

The private keys with which certificates can be signed, cannot be used after the end of their life cycle. The UZI register arranges adequate destruction to ensure that it is impossible to reproduce the destroyed keys from the remnants.

6.2.11 Cryptographic Module Rating

The Hardware Security Modules used within the UZI register systems have been certified in accordance with FIPS 140-2 level 3. As a consequence, cryptographic material cannot be changed during storage, use and transport without this being noticed. The supplier will supply the HSMs in tamper-evident bags so that any form of interference can be detected. Each consignment is checked immediately upon arrival, on the basis of the corresponding out-of-band list.

The smart card (combination of microprocessor and operating system) is independently certified on the basis of the following standards:

- EN 419211-2:2013, Protection Profiles for secure signature creation device – Part 2: Device with key Generation, V2.0.1.
- EN 419211-3:2013, Protection profiles for secure signature creation device – Part 3: Device with key import, V1.0.2.

6.3 Other aspects of key pair management

All aspects of the key management are executed by the UZI register through the application of careful procedures which correspond to the intended purpose.

6.3.1 Public key archival

Public keys are archived by the UZI register for at least seven years after the end of the original period of validity of a certificate, in a physically secure environment.

6.3.2 Certificate operational periods and key pair usage periods

Table 5 Validity CA Certificate Public G3/Private G1 hierarchy gives an overview of the validity period of the Public G3 / Private G1 hierarchy.

Table 5 Validity CA Certificate Public G3/Private G1 hierarchy

Certificate	Valid until
Root Certificate	November 14, 2028
Domain certificate	November 13, 2028
TSP certificate	November 12, 2028

For the certificates on the UZI card, including the associated key pairs, a maximum period of three years from the production date is used. For certificates in the server certificates, a maximum period of three years after the production date is used. The production date is the date on which the Certification Authority (CA) produced and published the certificate.

6.4 Activation data

6.4.1 Activation data generation and installation

The use of activation details is linked to the use of a smart card. These activation details are prepared and distributed in a safe manner. Distribution always takes place separately from the UZI card. The PIN and the PUK code consist, in all instances, of a minimum of six numbers. The PIN and the PUK code are only made available to the certificate holder and are only issued once.

One-time activation
Passes produced after 01/24/2021 are equipped with a QSCD chip and must be activated due to security requirements before they can be used.
The PIN code and Safesign software version 3.5.6.1 or higher are required for activation. It is important that this activation is a one-off and deliberate action by the certificate holder. If the certificate holder receives a message upon activation that the card has already been activated and he / she has not done this before, one should find out why and NOT use the card.

6.4.2 Activation data protection

Activation details are distributed in such a way that it is impossible for third parties to access the details without being detected. After transfer of the activation details, the certificate holder will be responsible for protecting these details.

If the cardholder did not receive the first PIN letter, it can be reprinted and sent again by the UZI register. The PIN letter can only be reprinted if the UZI card has already been issued. Reprinting of the PIN letter is only possible for a period of 6 weeks after the card has been issued. Given that the initial activation details may have been issued to a different person, the cardholder must change the PIN and PUK code immediately after receipt.

After the period of 6 weeks, the UZI register will assume that the activation details have been correctly received. The cardholder is responsible for monitoring this deadline. The UZI register will charge the normal rate for a new card with new codes. If the subscriber is to blame for the PIN letter being sent to the wrong address, for example because the UZI register was not informed in time of a change of address or if the cardholder/subscriber lost the PIN letter, the subscriber will receive an invoice for the costs of resending the PIN letter.

In the event of a reprint the UZI register will, for security reasons, generate a new revocation code.

The option of reprinting must not be used if the cardholder received the PIN letter but then lost it. For security reasons a new card must then be applied for. Normal charges apply for a new card with new codes.

6.4.3 *Other aspects of activation data*

The UZI card will be blocked after an incorrect PIN has been entered for a third time. Unblocking can be done using a PUK code. If the PUK code is also incorrectly entered three times, the smart card will be blocked for good and therefore rendered unusable. The PIN and the PUK code will be communicated to the certificate holder

in a PIN letter. In the event that the codes are lost, it will no longer be possible to use or unblock the card. Normal charges apply for a new card with new codes.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The registration systems of the UZI register include suitable checks and security measures. Partly for this reason it is impossible for a card application to be processed by a single employee of the UZI register.

The UZI register will take adequate measures to safeguard availability, integrity and exclusivity. Computer systems will be secured in a suitable manner against unauthorised access and other threats. The UZI register has an information security plan which details the measures in question. The measures will be developed into service level agreements with suppliers. Management activities will be logged.

6.5.2 Computer security rating

The UZI register classifies the resources used on the basis of a risk analysis.

6.6 Life cycle technical controls

6.6.1 System development controls

An independent EDP auditor has issued an audit certificate for the systems used by the UZI register on the basis of CEN TS 419 261:2015 or EAL 4+ certificate in accordance with ISO/IEC 15408. The UZI register carries out tests before the systems are put to use. Testing takes place in accordance with test plans drawn up in advance.

6.6.2 Security management controls

The UZI register has separate test, acceptance and production systems. The transfer of software from one environment to another takes place in a controlled fashion via a change management procedure. This change management procedure covers, among other things, monitoring and recording versions, changes and emergency repairs to all operational software.

The integrity of TSP systems and information is protected against viruses, malware and unauthorised software and other possible sources that could lead to a disruption of the services, by means of a combination of suitable physical, logical and organisational measures. These measures are preventive, repressive and corrective in nature. Examples of these measures are logging, firewalls, intrusion detection and redundancy of systems, system elements and network components.

All used system storage media are treated safely in order to protect them from damage, theft and unauthorised access. Storage media are carefully removed when they are no longer needed.

Usage capacity is monitored and predictions are made in order to ensure sufficient processing capability and storage capacity in the future.

6.6.3 Life cycle security controls

The security classification is assessed annually and modified as necessary.

6.7 Network security Controls

Measures have been implemented for network security in such a way that safeguards the availability, integrity and exclusivity of the details.

Communication about public networks between systems of the TSP takes place in a confidential manner.

The link between the public networks and the networks of the UZI register is subject to stringent safety measures (up-to-date firewall, virus scanners, proxy).
These controls include a monthly security scan and a (minimum) annual penetration test.

6.8 Time-stamping

No stipulation

7 Certificate, CRL and OCSP profiles

7.1 Certificate profile

This section provides an overview of the certificate profile of the UZI register. In particular, the fields that contain relevant data for certificate holders are discussed.

An X.509 certificate consists of a collection of information objects. Each object has a name, and each object consists of a number of attributes. An attribute can contain various items such as keys, algorithms, names, etc. A certificate profile describes which objects are used and which values the attributes of these objects can contain.

The basic structure of a certificate consists of a to-be-signed section (tbsCertificate) and a signature of the issuer. The tbsCertificate consists of a number of obligatory basic attributes followed by extensions. The following subsections describe the basic attributes and extensions of the certificates issued by the UZI register.

7.1.1 Version number(s)

The UZI register certificates comply with the X.509 v3 standard and also comply with the following standards:

- Part 3a, 3b and 3h of the Programme of Requirements of the PKI for the Government (see https://www.logius.nl).
- In addition, the signature certificates are structured in accordance with the Qualified Certificate Profile of the relevant ETSI standards. The specific extensions in that context are also included in the signature certificates (non-repudiation) of the UZI register.

7.1.2 Certificate extensions

Basic attributes

The certificates from the UZI register have the following basic attributes insofar as they are not described in other paragraphs:

Table 6 Basic attributes of certificate profiles

Field	Value
Certificate. SerialNumber	Contains the unique serial number of the certificate
Validity	The certificate validity period for the certificates is set to three years

Standard extensions

The certificate contains the following standard extensions:

Table 7 Standard extensions of certificate profiles

Field	Essential	Value
AuthorityKeyIdentifier	No	KeyIdentifier is set to 160 bit SHA-1 hash of the public key of the CA that issued the certificate.
SubjectKeyIdentifier	No	KeyIdentifier is set to 160 bit SHA-1 hash of the public key of the subject

Field	Essential	Value
KeyUsage	Yes	Differs per certificate type: - In **authenticity certificates** only the digitalSignature bit is included. - In **confidentiality certificates** only the keyEncipherment and dataEncipherment bits are included. - In **signature certificates** only the non-Repudiation bit is included in a unique way. - In the **server certificates** (services) only the DigitalSignature and KeyEncipherment bits are included.
BasicConstraints	Yes	The CA bit is set to 'False' and pathLenConstraint to 'none'
CertificatePolicies	No	Contains: - the Object Identifier (OID) for the applicable Certificate Policy of the PKI for the Government (see section 7.1.6); - A link to the CPS of the UZI register (see section 1.2.3); - a user text (UserNotice) in Dutch that translates as 'The field of application of this certificate is limited to communication within the Government domain as indicated in the Program of Requirements of the PKI for the Government. See www.logius.nl'
AuthorityInfoAccess. accessMethod (OCSP)	No	This attribute includes the URL of the OCSP services: http://ocsp.uzi-register.nl.
AuthorityInfoAccess.accessMethod (CA Issuers)	No	In this attribute the URL is included to CA certificate of the issuing CA. This varies per product: - http://cert.pkioverheid.nl/UZI-register_Zorgverlener_CA_G3.cer - http://cert.pkioverheid.nl/UZI-register_Medewerker_op_naam_CA_G3.cer - http://cert.pkioverheid.nl/UZI-register_Medewerker_niet_op_naam_CA_G3.cer - http://cert.pkioverheid.nl/UZI-register_Private_Server_CA_G1.cer The TSP CA's issued under the G3 CA hierarchy are 'resigned' April 18th, 2019 and used in production since June 1st, 2019. Since this date the CaIssuers URL's in end certificates are as follows: - http://cert.pkioverheid.nl/20190418_UZI-register_Zorgverlener_CA_G3.cer - http://cert.pkioverheid.nl/20190418_UZI-register_Medewerker_op_naam_CA_G3.cer - http://cert.pkioverheid.nl/20190418_UZI-register_Medewerker_niet_op_naam_CA_G3.cer

Field	Essential	Value
ExtendedKeyUsage	No	ExtendedKeyUsage is essential in authenticity certificates in order to be able to use the certificate for smart card logon. The following values are included: - clientAuth: certificate usable for SSL client authentication - email protection. This is needed to be able to use the certificate in standard email clients - documentSigning so that the certificate is usable for signing documents The signature certificates include the following ExtendedKeyUsages: - email protection. This is needed to be able to use the certificate in standard email clients - documentSigning so that the certificate is usable for signing documents The confidentiality certificates include the following ExtendedKeyUsages: - email protection. This is needed to be able to use the certificate in standard email clients - Encrypting File System. This is necessary for the encryption of system files. Server certificates include the following ExtendedKeyUsages: - ServerAuthenticatie - ClientAuthenticatie
SubjectAltName	No	This attribute includes various numbers in the subjectAltName.otherName which may have a meaning within the care sector and which uniquely identify the subject as a care provider within a certain care institution. The authenticity certificate includes a separate subjectAltName.otherName with a Microsoft User Principal Name (UPN) to make the certificate suitable for smart card logon. The UPN is filled in with the following value: <UZI number>@<subscriber number>
CrlDistributionPoints	No	Contains the URI by which the CRL in question, which belongs to the certificate type, can be retrieved: - http://www.csp.uzi-register.nl/cdp/uzi-register_zorgverlener_ca_g3.crl - http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_op_naam_ca_g3.crl - http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_niet_op_naam_ca_g3.crl - http://www.csp.uzi-register.nl/cdp/uzi-register_private_server_ca_g1.crl

Clarification subjectAltName.otherName

This section describes how the subjectAltName.othername is included in the certificates from the UZI register.

PKI overheid specifies a subjectAltName.othername with an OID-like structure, as follows: **<OID CA>-<Subject ID>.** The <OID CA> and the <Subject ID> are separated by a '-'.

<OID CA>

stands for the OID of the issuing CA, which represents
<PKIoverheid>.<Domain>.<TSP>.<CA>.

Values SubjectAltName.otherName: <OID CA>
The following table shows the values of the <OID CA> in the production environment.

Table 8 <OID CA> production environment UZI register

CA type	OID
UZI register Care Provider [zorgverlener] CA	2.16.528.1.1003.1.3.5.5.2
UZI register named employee [medewerker op naam] CA	2.16.528.1.1003.1.3.5.5.3
UZI register unnamed employee [medewerker niet op naam] CA	2.16.528.1.1003.1.3.5.5.4
UZI register Server CA	2.16.528.1.1003.1.3.5.5.5

<Subject ID>
is a specific identification within the domain of the TSP. In this the UZI register has chosen to include various numbers which may have a meaning within the care sector and which uniquely identify the subject as a care provider within a certain subscription.

Values SubjectAltName.otherName: <Subject ID>
The <Subject ID> in the UZI register is a compound field, consisting of fields separated by a '-':

<Subject ID> = <version no.>-<UZI no.>-<card type>-<Subscriber no.>-<role>-<AGB code>

The following table clarifies the fields:

Table 9 Fields <Subject ID> in SubjectAltName.otherName

Field	Type	Value	Explanation
version no.	1NUM	1	Version number of the <Subject ID> specification for possible future developments.
UZI no.	9NUM	See par 7.1.4.	A unique number for certificate holders.
card type	1CHAR	The following coding is used: 'Z' : Care provider card [zorgverlenerpas] 'N' : Named employee card [medewerkerpas op naam] 'M' : Unnamed employee card [medewerkerpas niet op naam] 'S' : Server Certificates	Coding for type of UZI resource.
Subscriber no.	8NUM		Subscriber number of the care provider or indication body.
role	6CHAR	Depending on card type For care provider cards [zorgverlenerpassen] <professional title code>.<specialism code> The <professional title code>=2NUM The <specialism code>=3NUM **OR**	In the case of the care provider card [zorgverlenerpas] the <professional title code> always has a value which is not equal to zero. The <specialism code> may be zero because a lot of professional titles do not have a specialism and it is not

Field	Type	Value	Explanation
		'00.000' For named employee card [medewerkerpas op naam], unnamed employee card [medewerkerpas niet op naam] and Server Certificates	obligatory to include the specialism. For further clarification on filling-in, see Annex 3.
AGB code	8NUM	AGB code or 00000000 if no AGB code given.	See table 11

Clarification value AGB-code
An AGB code can be included in the card or server certificates upon request. In consultation with Vektis it has been decided which AGB code is to be included per card.

Table 10 Clarification of AGB code use

Card type \ Subscriber type	Care provider [zorgverlener]	Organisation
Care provider [zorgverlener]		
Named employee [medewerker op naam]	AGB care provider code subscriber [zorgverlenercode abonnee]	AGB code practice or institution
Unnamed employee [medewerker niet op naam]	AGB care provider code subscriber [zorgverlenercode abonnee]	AGB code practice or institution
Server	AGB care provider code subscriber [zorgverlenercode abonnee]	AGB code practice or institution

Private extensions
The certificate contains the following private extensions.
Non-repudiation certificates contain very few qcStatements which indicate that the certificate in question is a qualified certificate.

Table 11 Private extensions certificate profiles

Field	Essential	Value
etsiQcsCompliance	No	Indicates that the issue of a qualified certificate corresponds with Annex I of EU Regulation 910/2014.
etsiQcsQcSSCD	No	Indicates that the private key belonging to the public key has been stored in the certificate on a qualified signature-creation device (QSCD) in accordance with Annex II of EU Regulation 910/2015.
etsiQcsQcType (Type1)	No	Indicates type of qualified certificate in accordance with Annex I of EU Regulation 910/2014. Type 1: Certificate for electronic signatures (esign) as defined in Regulation (EU) No 910/2014
etsiQcsQcPDS	No	Reference to PKI Disclosure Statement (PDS) with https://www.zorgcsp.nl/pds/pds.html as the URL and English as the language.

Email addresses
The email address is not included in the certificate profiles for the UZI register.

7.1.3 Cryptographic algorithm object identifiers
The certificates of the UZI registry are signed with the algorithm sha256WithRSAEncryption (Object Identifier 1.2.840.113549.1.1.11).

The certificates contain an RSA key of at least 2048 bits.

7.1.4 Name forms

Certificates issued by the the UZI register contain the name of the CA that signs the certificate (issuer) and of the certificate holder (subject) as shown in the following table.

Field	Value
Issuer	Contains the name of the UZI register CA in question belonging to the type of UZI card and is displayed using the OrganizationName, organizationIdentifier, CommonName and CountryName attributes. The **OrganizationName** is 'CIBG' De **organizationIdentifier** is 'NTRNL-50000535' The **CommonName** contains one of the following values depending on the card type: - 'UZI register Care Provider [zorgverlener] CA G3' - 'UZI register named employee [medewerker op naam] CA G3' - 'UZI register unnamed employee [medewerker niet op naam] CA G3' - 'UZI register Private Server CA G1' The **CountryName** is set to 'NL' in accordance with ISO 3166.
Subject	The name of the subject is shown as a Distinguished Name (DN), and by the following attributes which are included in all certificates: CountryName, CommonName, OrganizationName, and SerialNumber. The attributes which are used to describe the subject define the subject in a unique way. The **CommonName** contains: - for the care provider card [zorgverlenerpas] and named employee card [medewerkerpas op naam], the full name of the certificate holder: <first names><space><if filled in: prefixes birth name+ space><birth name>; - for the unnamed employee card [medewerkerpas niet op naam], the function of the employee as indicated by the subscriber; - for the Server Certificates the name of the system, the so-called fully qualified domain name (FQDN). The **OrganizationName** contains the name of the subscriber. This is the party on whose behalf the certificate holder acts when using the certificate. The **CountryName** contains the country of the subscriber in accordance with ISO 3166. The **SerialNumber** contains the UZI number (See section 7.1.4). In addition to the above attributes which are always present, Title, Surname, GivenName, StateOrProvinceName, LocalityName and OrganizationalUnitName are also in use, but not for all types of certificates. The **Title** attribute contains, for the care provider card [zorgverlenerpas], the formal term of address (role) of the care provider [zorgverlener] (e.g. dentist [tandarts] or cardiologist [cardioloog]). More information about filling-in this field is included in Annex 3. In the case of the care provider card [zorgverlenerpas] and the named employee card [medewerkerpas op naam], the **Surname** and **GivenName** are also used.

Field	Value
	These contain respectively <if filled in: prefixes birth name+ space><birth name> and the <first names>. The **OrganizationalUnitName** only occurs as an option in the case of the unnamed employee card [medewerkerpas niet op naam] and Server Certificates, and offers space for including the department of the employee or server. Server Certificates include the **StateOrProvinceName** which contains the name of the state or province where the subscriber is located and the **LocalityName** which contains the name of the neighbourhood or local area where the subscriber's business is located.

Clarification UZI-number
In the certificate profile of the UZI register the UZI number is included in the subject.SerialNumber of all types of card of the UZI register. This guarantees that the subject Distinguished Name is unique.

For the 'care provider' [zorgverlener] and the 'named employee' [medewerker op naam] cards, the UZI number is uniquely linked to the natural person. Any new card application for the same natural person, will contain the same UZI number. If a 'care provider' [zorgverlener] or 'named employee' [medewerker op naam] applies for cards for various institutions, these cards will contain the same UZI number. A person will only be issued with a new UZI number if his/her first names, (prefixes) birth name, date of birth or birthplace change.

In the cases of unnamed employee [medewerkerpas niet op naam] and Server Certificates, a new unique UZI number is generated with each (card)application/(card)issue. The UZI number on this card type offers trusting parties the possibility to check with the subscriber in question as to which employee or system is involved. Whenever a card is applied for, a new UZI number will be generated because the UZI register cannot issue a guarantee that the same employee or service is involved. A record of this is kept by the subscriber.

The UZI register will generate the UZI number for all types of card using the same nine-digit number series.

7.1.5 Name constraints
For the names in certificates, the preconditions arising from RFC 5280, ETSI EN 319 411-1 and ETSI EN 319 411-2 and the Program of Requirements PKIoverheid apply.
The following name fields of a care provider card and a named employee card may be longer than the upper bounds specified in RFC 5280:
- GivenName up to 50 characters;
- Surname up to 65 characters;
- CommonName up to 116 characters.

7.1.6 Certificate policy object identifier
For the Certificate Policies (CP) reference is made to https://www.logius.nl. In order to be able to identify the correct CP, the following table shows the relationship between the cards, the functions of the certificates, the applicable CP and the Object Identifier (OID) of the CP. The OID CP column contains the Object Identifier that is included in the certificates and that unambiguously refers to the Certification Policy (CP) that applies to the certificate in question.

Table 12 Overview of certificates with OID of applicable CP Public G3/Private G1 generation

Type of certificate		**Applicable CP**	**OID CP**
UZI Card	**Certificate (function)**		
Care provider [zorgverlener] Named employee [medewerker op naam]	authenticity	SoR section 3a, Certificate Policy – Organisation Domain (G3)	2.16.528.1.1003.1.2.5.1
	signature (non-repudiation)	SoR section 3a, Certificate Policy – Organisation Domain (G3)	2.16.528.1.1003.1.2.5.2
	confidentiality	SoR section 3a, Certificate Policy – Organisation Domain(G3)	2.16.528.1.1003.1.2.5.3
Unnamed employee [medewerker niet op naam]	authenticity	SoR, section 3b, Certificate Policy – Services, Organisation Domain(G3)	2.16.528.1.1003.1.2.5.4
	confidentiality	SoR, section 3b, Certificate Policy – Services, Organisation Domain (G3)	2.16.528.1.1003.1.2.5.5
Server	authenticity and confidentiality	SoR, section 3h, Certificate Policy – Services, Organisation Domain(G1)	2.16.528.1.1003.1.2.5.6

7.1.7 Usage of Policy Constraints extension
No stipulation.

7.1.8 Policy qualifiers syntax and semantics
As indicated in section 7.1.2 the 'CertificatePolicies' extension contains two Policy Qualifiers:
- a link to the UZI register CPS (see section 1.2.3);
- UserNotice (see section 7.1.2)

7.1.9 Processing semantics for the critical Certificate Policies Extension
No stipulation.

7.2 CRL profile

The CRL profile is compiled in accordance with section 3a, 3b and 3h of the Programme of Requirements of the PKI for the government (see https://www.logius.nl). The profile of the CRL for the certificates contains a number of attributes and extensions. These are shown in the following subparagraphs.

7.2.1 Version number(s)
The UZI register issues CRLs according to the X.509 version 2 format.

7.2.2 CRL and CRL entry extensions
The CRLs for certificates from the UZI register have the following attributes.

Table 13 CRL profile

Field	Value
Version	1 (X.509 version 2)
signatureAlgorithm	SHA-256 WithRSAEncryption

Field	Value
Issuer	Contains the name of the UZI register CA belonging to the certificate type and is displayed using the following attributes: OrganizationName, CommonName, , organizationIdentifier and CountryName. The OrganizationName is set to 'CIBG' De organizationIdentifier is 'NTRNL-50000535' Depending on the CA that signs the CRL, the CommonName contains: 'UZI register Care Provider [Zorgverlener] CA G3' 'UZI register named employee [Medewerker op naam] CA G3' 'UZI register unnamed employee [Medewerker niet op naam] CA G3' 'UZI register Private Server CA G1' The CountryName is set to 'NL' in accordance with ISO 3166.
thisUpdate	Date/time of issue.
nextUpdate	This is the date/time when the validity of the CRL ends. The value is 'thisUpdate' plus forty- eight hours. The UZI register publishes an update of the CRL every hour.
revokedCertificates	The revoked certificates per entry: - certificate serial number - date/time of revocation

The CRLs for certificates from the UZI register have the following extensions:

Table 14 CRL extensions

Field	Essential	Value
AuthorityKey Identifier	No	Contains 160 bit SHA-1 hash of the public key of the CA that signed the CRL.
CRLNumber	No	Sequence number
ExpiredCerts OnCRL	No	Indicates that revoked certificates remain on the CRL after the certificate expires in accordance with ETSI EN 319 411-2: CSS-6.3.10-05

7.3 OCSP profile

7.3.1 Version number(s)

The OCSP service of the UZI register is of the type 'pkix-basic', complies with RFC 6960 and has the following characteristics:

- The OCSP service does not use pre-computed responses.
- All OCSP communication for UZI register certificates uses the URL http://ocsp.uzi-register.nl
- Each CA of the UZI registry that issues user certificates has its own OCSP responder that signs the OCSP responses with its own private key. So in total there are 4 OCSP signers: one for each CA/product type;
- The OCSP responder certificates follow the certificate profile for server certificates wherever possible. Specific deviations in the OCSP responder certificate profiles are:
  - the lack of Subject.StateOrProvinceName, Subject.Locality and Subject.Serialnumber
  - the lack of the Authority Information Access
  - the lack of the Subject.AltName
  - the subject.CommonName is as follows: OCSP responder [CN delegated CA]. For example, for the 'UZI register Care Provider [zorgverlener] CA G3', the

CN of the corresponding OCSP responder is: 'OCSP responder UZI register Care Provider [zorgverlener] CA G3'.
- the use of KeyUsage=Digital Signature
- the use of extendedKeyUsage=id-kp-OCSPSigning
- the use of a so-called ocsp-nocheck extension (Object Identifier 1.3.6.1.5.5.7.48.1.5)

7.3.2 OCSP extensions

The OCSP responses of the UZI register have the following characteristics:
- a version number of the response syntax;
- an ID of the responder;
- a response for each of the certificates in the request as explained in more detail below;
- the period of validity of the response;
- optional extensions, currently only the OCSP Nonce;
- an OID that indicates the signature algorithm used: sha256WithRSAEncryption;
- a signature of the response;
- the certificate to validate the signature under the response.

For each of the certificates in a request the response contains:
- a certificate identifier;
- the certificate status that has one of the following three values:
  - 'Good'
  - 'Revoked'
  - 'Unknown'

The status 'good' indicates, as a minimum, that the certificate has not been withdrawn, but does not guarantee that the certificate is still valid at that point in time. The 'revoked' status indicates that the certificate has been revoked. The 'unknown' status indicates that the OCSP responder of the UZI register does not know the status of the certificate. This could occur, for example, if the status of a test certificate is requested from the OCSP responder of the production environment.

8 Compliance audit and other assessments

The TSP service of the UZI register was certified in 22-11-2004 on the basis of the 'Scheme for certification of Certification Authorities' based on ETSI EN 319 411-2 and ETSI TS 102 042. As it still holds this certification, it fulfils the requirements imposed on certification service providers in ETSI EN 319 411-2 and the requirements contained in the Electronic Signatures Act [Wet elektronische handtekeningen] (Weh). The ETSI TS 101 456 standard has been superseded by ETSI EN 319 411-2 (in combination with ETSI EN 319 401). ETSI 102 042 has been superseded by 319 411-1 as of 1 July 2016.

eIDAS
On 1 July 2016, the European Regulation (Regulation (EU) no. 910/2014 of the European Parliament and the Council of 23 July 2014 concerning electronic identification and trust services for electronic transactions in the internal market and implying revocation of Directive 1999/93/EC) came into effect.
This regulation replaces the Electronic Signatures Act [Wet elektronische handtekeningen].
Because this regulation includes the requirements with regard to frequency of the audit and the accreditation, the TTP.NL Scheme is no longer valid as of that date.

In addition, the earlier ETSI certifications in November 2016 ETSI TS 101 456 and ETSI TS 102 042 have been replaced by the ETSI certifications ETSI EN 319 411-2 and ETSI EN 319 411-1 respectively.

The UZI register also complies with the relevant elements of the Programme of Requirements of the PKI government as stipulated in the Programme of Requirements. This can be demonstrated using an audit certificate issued by BSI Group The Netherlands B.V.

A copy of the ETSI EN 319 411-1 and the ETSI EN 319 411-2 certificates can be found on the site of the UZI register (see certification policy).
For reasons of secrecy the audit reports drawn up by the auditors in question are confidential. They are not available to third parties and may only be perused on request and in strict confidentiality.

As from 10 March 2017, the Radio Communications Agency Netherlands [Agentschap Telecom] (hereafter referred to as AT) has been designated as the legal regulator for eIDAS regulation. As Trust Service Provider (TSP) the UZI register has been registered under registration number 940473 with the Radio Communications Agency Netherlands, as verified issuer of Qualified Certificates to the public.

8.1 Frequency or circumstances of assessment

The audit cycle is performed in accordance with the ETSI EN 319 403 certification schedule. The UZI register undergoes a certification audit once every 2 years. In the interim years a full verification audit is carried out every year. If larger changes are implemented at a policy or technical level, an interim conformity audit can be carried out.

Besides these audits the UZI register also carries out internal audits and self-assessments.

8.2 Identity/qualifications of assessor

Certification audit and verification audits are performed by an organisation accredited by the Dutch Accreditation Council.

8.3 **Assessor's relationship to assessed identity**

The auditors that perform the audits are independent. There is no additional relationship between the UZI register and the certifying body.

8.4 **Topics covered by assessment**

During the audits, an assessment is carried out to determine to what extent the management system for the issuing of (qualified) certificates permanently fulfils the requirements of the standards:

- ETSI EN 319 411-1, (with respect to the unnamed employee card [medewerkerpas niet op naam] and Server Certificates), including the standards referred to therein of the CABforum Baseline Requirements and the Network Security Controls.
- ETSI EN 319 411-2, (with respect to the care provider card [zorgverlenerpas] and named employee card [medewerkerpas op naam])
- requirements from the Regulation on electronic identification and trust services (the eIDAS Regulation)
- the Programme of Requirements PKI government parts 3a, 3b and 3h.

The audit is performed on the following issues and processes:

- Registration Service.
- Certificate Generation Service.
- Dissemination Service.
- Revocation Management Service.
- Revocation Status Service.
- Subject Device Provision Service.

8.5 **Actions taken as a result of deficiency**

If shortcomings are discovered during the audit, the UZI register draws up, within 3 weeks after receipt of the audit report, an action plan to analyse the observed deviations and take effective corrective measures.

8.6 **Communication of results**

The conformity certificates of the most recent audits will be available on the website of the UZI register and in the electronic storage location of the Policy Authority of the PKI for the government. The UZI register also complies with the framework of standards of the PKI for the government as stipulated in the Programme of Requirements (see www.logius.nl).

9 Other business and legal matters

9.1 **Fees**

9.1.1 Certificate issuance or renewal fees

The application of UZI certificates, namely the Server Certificate and the UZI card, from a Care Provider [zorgverlener] (subscriber) registered in the UZI register, is subject to a cost-covering rate. This rate is applicable to both the initial application and subsequent applications for an UZI certificate, including renewals. The rates for the UZI certificates are stated on www.uziregister.nl.

No costs are charged for rejected applications.

9.1.2 Certificate access fees

The UZI register does not charge any fees for certificate access.

9.1.3 Revocation or status information access fees

The UZI register does not charge any fees for revocation or status information access.

9.1.4 Fees for other services

A fee may be charged for a reprint of the PIN code letter, see section 6.4.2

9.1.5 Refund policy

In accordance to Article 6, lid 3 of the Regulation on the Use of the Citizen Service Number in Healthcare [Regeling gebruik burgerservicenummer in de zorg], restitution of paid fees is not possible, unless in the opinion of the Minister of Health, Welfare and Sport there is a circumstance that cannot be attributed to the person for the benefit of who produced the card or certificate

9.1.6 Rate changes

The rate for the UZI certificates may change periodically. If the rate is changed, the Regulation on the Use of the Citizen Service Number in Healthcare [Regeling gebruik burgerservicenummer in de zorg] will be changed accordingly and notification of this change will be given on www.uziregister.nl.

9.1.7 Invoicing and payment

Within three weeks after the production date of the UZI card, the subscriber will receive an invoice at the postal address registered with the UZI register. In addition, the invoice will be sent in digital form to the applicant's email address. The UZI register has outsourced the invoicing activities to Cannock Outsourcing B.V. The invoice will be sent out on the basis of the details issued to Cannock Outsourcing B.V., such as the postal address of the subscriber and the email address of the card applicant. The UZI register will not honour a request for a modification to an invoice.

The card applicant is responsible for choosing the right UZI certificate. If the card applicant applies for an UZI certificate which turns out to be incorrect, for example a wrong type of UZI card or wrong PKCS#10 file, the full costs will be charged.

9.1.8 Payment term

The payment term after invoicing is thirty days. In the event of late payment, the UZI register is entitled to instigate collection measures and/or engage a third party to collect the claim. In the event of late payment UZI certificates will be withdrawn by the UZI register. The revocation of UZI certificates will take place six weeks after the reminder has been sent.

9.1.9 Validity of UZI certificate

In accordance to Article 7 of the Regulation on the Use of the Citizen Service Number in Healthcare [Regeling gebruik burgerservicenummer in de zorg] the period of validity of an UZI certificate is three years after the production date. The production date is the date on which the Certification Authority (CA) produced and published the certificate.

9.1.10 Delivery and initial usage of UZI certificates

The UZI certificates are delivered in accordance with the technical and/or functional specifications referred to in the Certification Practice Statement (CPS). If it turns out that the UZI certificate does not function in accordance with the CPS, the subscriber or his authorized representative will immediately inform the UZI-register within six weeks after delivery of the UZI-card or after sending the UZI-server certificate.

9.1.11 Replacement conditions

If an UZI card or certificate does not work in accordance with the technical and/or functional specifications described in the CPS, the UZI register will replace it free of charge during the six weeks referred to in section 9.1.10.

The activation details (PIN and PUK code) can only be resent during the six weeks. See section 6.4.2 for the conditions and procedure.

If a certificate holder suspects that the UZI card is defective, the certificate holder must contact the Atos support desk[20]. If, following a telephone check by an employee of the support desk, it is established that the UZI card is probably defective, the subscriber may be eligible for the guarantee scheme. The subscriber can acquire a new card free of charge via this guarantee scheme. The guarantee scheme only applies if:

- The support desk has established, after a telephone assessment, that the card is probably defective.
- The UZI card is still valid for at least 3 months.
- The certificates on the UZI card are withdrawn by the subscriber, in accordance with the procedure in section 4.9.
- The subscriber or certificate holder returns the UZI card to the UZI register with the corresponding PIN and PUK codes. The subscriber is responsible for ensuring that the package is correctly received by the UZI register. It is therefore advisable to send it by registered post. These costs cannot be declared.
- On the basis of the notification and the UZI card received, the UZI register should be able to determine that the cardholder has used the card carefully. The card must not be visibly damaged upon receipt.

9.1.12 Risk, ownership and duty of care

The risk of destruction, loss or theft, damage or deterioration of UZI certificates transfers to the subscriber at the moment of receipt of an UZI certificate. The subscriber is not authorised to make any changes to the UZI certificate. The issued UZI certificates remain in ownership of the UZI register. The UZI register is authorised to withdraw an UZI certificate from use by a subscriber. UZI certificates cannot be transferred to third parties. The subscriber or authorised representative must ensure that the UZI certificates are used and stored in a careful, safe and prudent manner.

9.2 Financial Responsibility

20 The Atos service desk has been duly authorised by the CPS.

9.2.1 Insurance coverage
As a government organization, the CIBG cannot take out insurance and is therefore its own risk bearer. Agreements have been made with the ministry on risk policy. In the present cases, in cases of damage claims, the CIBG is liable to the maximum of its own (limited by agency regulations) assets. In addition, the Ministry (ie the owner / client) takes over the liability.

9.2.2 Other assets
No stipulation.

9.2.3 Insurance or warranty coverage for end-entities
No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information
On the basis of the Government Information (Public Access) Act [Wet openbaarheid van bestuur] (Wob) anyone can ask the UZI register to submit documents relating to a governmental matter.

If the UZI register outsources work to third parties, this work will be carried out under the responsibility of the UZI register. The agreements between third parties and the UZI register are laid down in contracts.

9.3.2 Information not within the scope of confidential information
No stipulation.

9.3.3 Responsibility to protect confidential information

If the issuing of documents or details could harm the services of the UZI register, the purchasers of its services, or one of the third parties engaged by the UZI register, these will not be made available to others, except those parties who need access to those documents in connection with their work. Examples of such documents are those that contain company-sensitive information in relation to infrastructure, security and finances.

9.4 Privacy of Personal Information

9.4.1 Privacy plan
A record will be kept of all activities carried out which are important in the registration process. During the process as few personal details will be recorded as possible. In any event no (personal) details will be recorded which are not important for the registration process or for one of the facilitating services of the UZI register.

The authorised applicants, certificate holders and certificate managers are entitled to meet and correct their personal details.

9.4.2 Information treated as private
The information obtained by the UZI register about a person, being a natural person or legal identity, will be treated as confidential. The requirements imposed in the General data protection [Algemene verordening gegevensbescherming] (AVG) are explicitly applicable.
At least the following documents contain information which is regarded as confidential and will therefore, in principle, not be issued to third parties:

- information relating to the registration and certification of parties;
- agreements with suppliers and service providers;

- security procedures and measures;
- Administrative Organisation (AO) procedures;
- audit reports.

9.4.3 Information not deemed private
The published details of certificates can only be consulted publicly using the search function on the website. The information issued in relation to published and withdrawn certificates is limited to that referred to in chapter 7 'Certificate, CRL and OCSP profiles' of this CPS.

Information in relation to revocation of certificates is available via the CRL. The information provided there relates only to the certificate number, the moment of revocation and the status (valid/withdrawn) of the certificate.

9.4.4 Responsibility to protect private information
CIBG has the responsibility to protect private information.

9.4.5 Notice and consent to use private information
Confidential details will only be issued in order to provide proof to parties other than the subscriber or certificate holder, on the basis of the prior written permission of the subscriber or the certificate holder.

9.4.6 Disclosure pursuant to judicial or administrative process
If, within the framework of a criminal or disciplinary legal investigation, non-public information is requested from the UZI register by an authorised investigating officer, this information will be released by the director of the CIBG on the basis of a court order. The requirements imposed in the AVG are explicitly applicable to this.

If a subscriber or certificate holder requests non-public information from the UZI register in a civil procedure for the purposes of proof of certification, this information will be released by the director of the CIBG if, in the opinion of the latter, there is no substantial interest that stands in the way of the data issue. If data is going to be issued, the party in question will be informed accordingly.

9.4.7 Other information disclosure circumstances
Notwithstanding the above, no details belonging to certificate holders or subscribers will be released to third parties, unless this is necessary on the basis of legislation and regulations or if the subscribers or certificate holders have given their explicit permission.

9.5 **Intellectual Property rights**
This CPS is owned by the UZI register. Unchanged copies of this CPS may be distributed and published without permission provided the sources are mentioned.

Certificates and bearers of the private and public key (UZI card) issued by the UZI register certificates will continue to be the property of the UZI register. UZI cards must be returned at the request of the UZI register. All intellectual property rights related to the certificates and the UZI card, including the rights relating to software, databases and logos are vested in the UZI register. The rights cannot be transferred to third parties.

The UZI register guarantees its subscribers and certificate holders that the certificates and bearers of the private and public key it issues, including the corresponding and delivered equipment and documentation, do not violate intellectual property rights, including copyrights, brand rights and rights to software used which are vested in its suppliers.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

In its capacity as certificate service provider the UZI register is liable for damage which natural persons or legal entities, that reasonably trust a certificate issued by the UZI register and act on the grounds thereof, suffer in conjunction with:

- The accuracy, at the time of issue, of all the details included in the certificate and the inclusion of all details prescribed for this certificate.
- The fact that, at the time of issue, the party referred to in the certificate as signatory was the holder of the details for the generation of electronic signatures.
- The fact that the details for generating electronic signatures and the details for verifying electronic signatures, if both have been generated by the UZI register, can be used complementarily.

The UZI register can be held liable if it fails to register revocation of the certificate, including the updating and publishing of the CRL, and a person has acted accordingly in reasonable trust. The UZI register cannot be held liable, on the basis of the above grounds, if it can submit proof that no careless actions were taken.

The UZI register excludes all liability for damage if the certificate is not used in accordance with the usage described in section 1.4.

On the instruction of the Policy Authority of the PKI for the government, the UZI register can include usage-related restrictions in a signature certificate, provided these restrictions are clear to third parties. The UZI register is not liable for damage which is the consequence of using a signature certificate in a way which is contrary to the restrictions stipulated by the Policy Authority.

The UZI register guarantees that procedures have been set up and measures implemented so that this CPS is complied with.

The UZI register does not accept any liability to the trusted party for damage it suffers, in whatever form, apart from exceptions referred to below:
The UZI register is, in principle, liable in those instances in which a trusted party sufferers damage, in accordance with EU Regulation No 910/2014 (eIDAS) Article 13 and applies to all certificates.

9.6.2 RA representations and warranties

See section 9.6.1

9.6.3 Subscriber representations and warranties

Subscribers and certificate holders are obliged to observe the stipulations of the UZI register in relation to the purchase of certification services as laid down in the CPS. They must also observe instructions communicated to them by the UZI register when the UZI cards are issued and/or made known to them at a later date.

Certificate holders within an organisation are also obliged to comply with instructions communicated to them by the subscriber. In the event of any contradiction in the instructions of both parties, the instructions of the UZI register will, in principle, take precedence over the instructions of the subscriber.

If subscribers of certificate holders do not comply with the stipulations, this may result in damage for the UZI register, the subscriber, certificate holders or third

parties. In such instances the subscriber will, in principle, be held liable for not complying with the stipulations. The following stipulations are supplementary to section 4.6.1 of this CPS.

- The subscriber will only and exclusively purchase certification services from the UZI register for its systems, databases and employees.
- The legal representative guarantees that he is legally authorised to connect the subscriber to the UZI register. In addition, the legal representative can designate one or more authorised representatives, referred to as the applicant(s), for whom the legal representative will have final responsibility. This applicant(s) will be charged, on behalf of the subscriber, with the actual execution of the applications for and revocation of UZI cards in accordance with the procedures of the CPS. If the subscriber registration of (the organisation of) the subscriber is to be deleted, only the legal representative will be authorised to do so.
- The subscriber is obliged to set up and execute a procedure on the basis of which the subscriber or the applicant(s) can check whether the intended certificate holders within the subscriber's organisation actually perform work for the organisation. If the subscriber is a certificate holder, the same procedure will apply.
- The subscriber guarantees that the intended certificate holder works within the organisation for whom UZI cards are being applied for and that the card application per individual certificate holder is complete, correct and authorised. The subscriber always has final responsibility for ensuring that the application is correct. If the subscriber is a certificate holder, the same procedure will apply.
- Before applying for an UZI card, the subscriber must inform the intended certificate holder within the organisation in writing about the exact conditions for using the UZI card. This means any restrictions regarding its use, the existence of a voluntary accreditation and the procedures for complaint handling and processing disputes. The above must be in accordance with the CPS. This information must be drawn up by the subscriber in writing and in language which is easy to understand. In addition, the subscriber must ensure that the intended certificate holder has actually read the applicable obligations and procedures from the CPS before the UZI register proceeds to issue an UZI card. In order to achieve this the subscriber will record the rights and obligations of the intended certificate holders within the organisation in writing and will ensure that the certificate holders within the organisation comply with the procedures, rights and obligations resulting from the CPS. If the subscriber is a certificate holder, the same procedure will apply.
- The subscriber is always responsible for the choice and (physical) protection of his software, equipment and telecommunications facilities and the availability of his information and communication systems, with which he can set up the electronic communication for himself and the certificate holders within the organisation. For example, the subscriber will take suitable measures to protect his system against viruses and other software containing inappropriate elements.
- The subscriber will issue correct, full and up-to-date details to the UZI register, including details of the certificate holders within the organisation for the generation and issue of certificates. The subscriber will report changes in address, organisation, organisation name, positions, contact persons or personal details of the subscriber or the certificate holders within the organisation, or other relevant changes, to the UZI register no later than 24 hours after the change in question has occurred.
- If the subscriber applies for server certificates, he will also be obliged to set up and execute a procedure on the basis of which the subscriber or the applicant(s) can check whether the system or database for which a server certificate is being applied, is actually used for the organisation.

- The subscriber and certificate holder cannot transfer rights and obligations resulting from the relationship with the UZI register to third parties, unless determined otherwise by the UZI register.
- The subscriber will himself ensure timely replacement close to the end of the period of validity, and an emergency replacement in the event of compromise and/or other types of calamities relating to the certificate or master certificates. The subscriber is expected to take adequate measures to ensure the continuity of certificate use.[21]

The above obligations for the subscriber or certificate holder will be recorded and, insofar as they can be designated as too unspecific, will be developed into UZI register guidelines and/or more detailed regulations. Insofar as the provisions relate to UZI cards for which a subscriber has applied on behalf of the certificate holder within the subscriber's organisation, the rights and obligations between the subscriber and the certificate holder will have to be mutually recorded in writing.

9.6.4 Relying party representations and warranties
No stipulation.

9.6.5 Representations and warranties of other participants
For representations and warranties o certificate holders see section 9.6.3.

9.7 **Disclaimers of Warranties**
In the event of system defects, service activities, or factors outside the control of the UZI, the UZI register will do all it possibly can to ensure that the services can be reached again as quickly as possible. The publication service will be available again, no later than within 24 hours. With this in mind a fallback scenario has been designed which is regularly tested. The UZI register is not responsible for the non-availability of the services due to natural disasters or other circumstances for which the UZI register cannot be held responsible.

9.8 **Limitation of liability**
The UZI register accepts no liability for damage that occurs in conjunction with natural persons or legal entities in the event of:

- Damage if the certificate is not used in accordance with the described field of application.
- Damage which results from use of the certificate whereby the restrictions indicated on the certificate are violated.
- Damage which arises due to restrictions on the use of the signature certificate being violated, on the condition that the UZI register communicates the restrictions in advance to third parties.
- Damage as a consequence of non-attributable failures in the fulfilment (force majeure), including among other things: delay and defects in the execution of work which can be attributed to non-technical malfunctions, such as transmission errors, equipment and system software malfunctions, defects in the equipment and software, intent, which includes fraud, illegal use of software, sabotage, theft of details and operating mistakes by third parties, errors by third parties resulting in network failure, a power cut, fire, lightning strike, substantial water damage, a break in the telephone cable, war-related violence, acts of terror, natural disasters and, more generally, causes which are unconnected to the reasonable care taken by the UZI register.
- Damage which arises due to subscribers, cardholders and/or trusting parties not fulfilling the obligations described in this CPS.

21 In the event of calamities affecting the UZI register, the Ministry of Health, Welfare and Sport will take adequate measures.

- Damage as a consequence of misuse, loss, theft or other disappearance of the certificate, the PIN, the PUK code, revocation code, bearer of the public and private key and the private key.
- Damage which arises due to the issue of a certificate on the grounds of incorrect information provided by the subscriber or cardholder, insofar as the UZI register could not, on the basis of the procedures and checks referred to in this CPS, reasonably have discovered that the information was incorrect.
- Damage as a consequence of the use of a certificate after the time of revocation of the certificate and publication on the CRL.
- Damage as a consequence of errors caused by the transfer of details by the subscriber and/or cardholder, the software, the equipment or telecommunication facilities used by the subscriber and/or cardholder.
- Damage as a consequence of a defect and/or incorrect information in the sent message, or in the sending or receipt thereof, which leads to serious damage such as physical injury, death or environmental damage, including but not limited to damage within the framework of using medical applications.
- Damage caused by the courier company (AMP Groep) delivering the UZI product or checks the identity of the certificate manager/holder outside the agreed time window.
- Damage caused by the courier company having been unable to carry out the correct identification of the certificate manager/holder due to the actions of the certificate manager / holder.

Insofar as the interests involved in the trust are disproportional compared to the level of reliability offered by the certificate, the trusted party will be regarded as not having trusted the certificate reasonably, even if the trusted party has fulfilled all other obligations.

9.9 **Indemnities**

Compensation will be available only if it can be irrefutably established that the UZI register can be held liable for the damage suffered.

9.10 **Term and Termination**

If one or more stipulations of this CPS are declared inapplicable by legal judgement or otherwise, this will not affect the validity and applicability of all other stipulations. In that case the parties will be bound by a stipulation with the same purport, wherever possible, which cannot be rendered invalid.

9.10.1 Term

The CPS is valid from the date of publication. The CPS is valid as long as the services of the UZI register continue, or until the CPS is replaced by a newer version. Newer versions will be designated by a higher version number (vX.xx). In the event of major changes, the version number will be increased by 1. In the event of editorial changes, the version number will be increased by 0.10. Newer versions are to be published on the website of the UZI register.

9.10.2 Termination

If one or more stipulations of this CPS are declared inapplicable by legal judgement or otherwise, this will not affect the validity and applicability of all other stipulations. In that case the parties will be bound by a stipulation with the same purport, wherever possible, which cannot be rendered invalid.

9.10.3 Effect of termination and survival

No stipulation.

9.11 **Individual Notices and Communications with Participants**
No stipulation.

9.12 **Amendments**

9.12.1 Procedure for Amendment
The currently valid CPS will be assessed and updated by the UZI register at least annually. Changes apply as of the moment that the new CPS is published and reported to the Policy Authority. The management of the UZI register is responsible for correct compliance with the procedure as described in section 9.11 and for the eventual approval of the CPS in accordance with this procedure.

9.12.2 Notification mechanism and period
No stipulation.

9.12.3 Circumstances under which OID must be changed
No stipulation.

9.12.4 Change and classification requests
Subscribers, certificate holders, trusted parties and any other interested bodies can submit a written change request supported by arguments. The UZI register can itself submit a change request, for example as a result of an internal review or audit, a change to the Programme of Requirements of the PKI for the government, changed legislation or suchlike. All change proposals are to be directly recorded. The UZI register will send a confirmation of receipt to the party submitting the request.

The TSP management and staff of the UZI register will classify the change requests. Where necessary, specialist legal or technical knowledge will also be consulted. During classification the urgency of the change request will also be determined. Changes to the CPS will be implemented in batches wherever possible.

9.12.5 Publication of changes
The UZI register publishes the CPS on the website: www.zorgcsp.nl. In addition, the CPS can be requested using the contact information referred to in section 1.5.1 'Contact details'. These requests can be made by telephone or in writing.

9.13 **Dispute Resolution Provisions**
If a conflict arises regarding the interpretation of the stipulations of this CPS, the CPS will indicate the interpretation of the UZI register stipulations. This interpretation must take account of the general objective of the UZI register. If this clarification does not produce a satisfactory result for the party/parties involved, the conflict will be submitted to a conflict mediator acceptable to all involved parties, before any other judicial or extrajudicial steps are taken. Agreements about the financing of this conflict mediation will be made at that point in time. If the above does not lead to a settlement of the dispute, it will be submitted to a competent court in The Hague.

In the event of complaints concerning services delivered by the UZI register, the complaint must be submitted in writing to the UZI register, for the attention of the Applications and Processing department head Registers & Knooppunten 1, stating as reference: 'Complaint'. The UZI register will then process the complaint in accordance with the CIBG complaints procedure, as stipulated in chapter 9 of the General Administrative Law Act [Algemene wet bestuursrecht] (Awb).

If a conflict arises between two purchasers of services offered by the UZI register, the department head of the UZI register can mediate, or designate an independent mediator, if the parties cannot reach agreement on the basis of mutual consultation.

9.14 **Governing Law**
The services of the UZI register and this CPS are subject to Dutch law.

9.15 **Compliance with Applicable Law**
The UZI register is a certificate service provider within the meaning of the Telecommunications Act. As a result, it is bound by all European and national legislation and regulations related to its capacity as a TSP and the services that it delivers. The above applies with due regard for the fact that the UZI register, as part of the CIBG, is an administrative body within the meaning of the Awb.

9.16 **Miscellaneous Provisions**
If one or more stipulations of the CPS are declared inapplicable by legal judgement or otherwise, this will not affect the validity and applicability of all other stipulations.

9.16.1 Entire agreement
No stipulation.

9.16.2 Assignment
No stipulation.

9.16.3 Severability
No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)
No stipulation.

9.16.5 Force Majeure
No stipulation.

Annex 1: Definitions and abbreviations

The definitions of the terms used were drawn up based on the following assumptions:

- In a number of cases, a decision was taken to use the English terms. The reason for this is that, often, there is no correct Dutch translation for the English term in question. If a Dutch term is used alongside an English term with the same meaning, both terms will be included in the list (the most usual term is included in the list followed immediately by the translation in italics).
- In the case of 'PKI terms' (PKI = Public Key Infrastructure), the terms will link up wherever possible with the general definitions used by the PKI for the government and in the specialist literature on this issue.

The glossary consists of three columns: Abbreviation, Term and Definition. The terms are arranged alphabetically based on the 'Term' column. In a number of cases clarification is provided immediately after the definition and, where applicable, the source of the information, with an empty line in between.

Table 15 Terms, definitions and abbreviations

Abbreviation	Term	Definition
	Subscriber	A care provider [zorgverlener] registered in the UZI register that purchases certification services from the UZI register. The subscriber is the party on whose behalf a certificate holder acts when using a certificate. The name and the subscriber number of the subscriber are stated in the certificate.
	Surname	The surname is the (correspondence) name as used on a daily basis by the person.
AT	Radio Communications Agency Netherlands [Agentschap Telecom]	Radio Communications Agency Netherlands is both the implementing body and the regulator of legislation and regulations in the field of telecommunications, Source: www.agentschaptelecom.nl
AGB	General Care Providers Database [Algemeen Gegevensbeheer Zorgverleners]	A database in which details of care providers [zorgverleners] are registered. In addition to general personal and practical information, this registration also includes details which are important for the communication between care providers [zorgverleners] and care insurers, particularly with regard to billing. AGB is administered by Vektis.
AP	Authority personal data (autoriteit persoonsgegevens)	The AP makes sure that personal details are used carefully and are protected and that privacy is also guaranteed in the future.
WLZ	Long-Term Care Act [Wet langdurige zorg]	The Long-Term Care Act is for people who need intensive care or supervision all day. For example, elderly people with advanced dementia or people with a serious mental, physical or sensory handicap.
	Asymmetric key pair	A public and private key which are linked to each other mathematically in such a way that, in a cryptographic calculation, they are each other's counterpart. Asymmetric key pairs are used for, among other things, the placement and verification of the electronic signature. See also 'Private key' and 'Public key'.
	Authentication	A process whereby someone's identity can be confirmed or with which the integrity and origin of submitted details can be verified. See also 'Authentication certificate', 'Authorisation' and 'Identification'.

Abbreviation	Term	Definition
	Authentication certificate	A certificate that should exclusively be used for authentication - or electronic identification.
	Authorisation	Granting someone the authority to carry out certain activities (for example: inspecting, modifying or processing details).
AVG	General data protection regulation [Verordening algemene gegevensbescherming.	The General Data Protection Regulation (AVG) has been applicable since 25 May 2018. This regulation ensures that the same privacy legislation applies throughout
	BIG register	Register of professionals in individual healthcare as referred to in Articles 3 and 34 of the Individual Healthcare Professions Act. See also: www.bigregister.nl
	BSN services	Citizen Service Number (BSN) services include: - the requesting and verifying of a Citizen Service Number, - the requesting of personal details - the Compulsory Identification Act [Wet op de identificatieplicht] (WID) check.
BSN	Citizen Service Number	The unique identifying number allocated to a natural person pursuant to the Citizen Service Number [General Provisions] Act [Wet algemene bepalingen burgerservicenummer].
	CA certificate	A certificate from a Certification Authority that contains, among other things, the public key and has been issued and signed by a higher CA.
CIBG	CIBG	The CIBG is an implementing body of the Ministry of Health, Welfare and Sport, that is charged with a number of legal implementation tasks. See also: www.cibg.nl
	Certificate	Electronic confirmation which links details for the verification of a certain person with details about the confidentiality and authenticity and/or electronic signature and therefore confirms the person's identity. A certificate is a publicly accessible document that is issued by a TSP and that contains a number of details checked by the TSP. A certificate contains at least: a) the notification that the certificate is being issued as a qualified certificate; b) the identification and the country of establishment of the issuing certificate service provider; c) the name of the signatory; d) space for a specific attribute of the signatory, that is stated as necessary, depending on the purpose of the qualified certificate; e) details for the verification of the signature which correspond to the details for generating the signature being checked by the signatory; f) the statement of the times at which the validity of the qualified certificate starts and ends; g) the identity code of the qualified certificate; h) the electronic signature of the issuing certificate service provider which fulfils the criteria of Article 15a, second paragraph, sections a to d, of Book 3 of the Dutch Civil Code; i) any restrictions concerning the use of the qualified certificate, and j) any limits relating to the value of the transactions for which the qualified certificate can be used.
	Certificate holder	A natural person or legal identity for whom a certificate has been issued and whose identity can be established using the certificate.
	Certificate manager	The role of certificate management is only important for products where the certificate holder is a system or a group/position, in other words for Server Certificates and named employee cards [medewerkerpas op naam]. In the case of these products, the UZI register has opted for the applicant

Abbreviation	Term	Definition
		of these products to also act as the certificate manager on behalf of the subscriber.
	Certificate profile	A description of the content of a certificate. Each type of certificate (signature, confidentiality, etc.) has its own content and description. This contains, for example, agreements regarding names, etc.
CP	Certificate Policy - *certification-policy*	A document with an itemised collection of requirements that indicates the frameworks within which the UZI register issues certificates. The CP is drawn up by the Policy Authority of the PKI for the government. By using the CP, among other things, certificate holders and trusting parties can determine how much trust they place in the UZI register.
CRL	Certificate Revocation List - *certificate revocation list*	A list of withdrawn (= revoked) certificates. The Certificate Revocation List (CRL) can be accessed and consulted by the general public. The list is made available by and under the responsibility of the UZI register. The CRL is itself also electronically signed by the CA of the UZI register.
	Certification services	The issuing, managing and revocation of certificates by certification service providers, as well as other services related to the use of electronic signatures, identity and confidentiality.
CA	Certification Authority	The part of the UZI register that arranges the signing of the certificates and that is trusted by end users.
CPS	Certification Practice Statement	A document that describes the procedures pursued, and the measures taken by, the UZI register regarding all aspects of the services. The CPS describes how the UZI register fulfils the requirements stipulated in the Certificate Policy (CP).
	Compromise	Any violation of the trust in the exclusive use of a component by authorised persons. Within the framework of the PKI for the government, the term component usually means the private key. A key is regarded as compromised in the event of: - Unauthorised access or suspected unauthorised access; - Lost or presumed to be lost private key or SSCD; - Stolen or presumed to be stolen private key or SSCD; - Destroyed private key or SSCD. A compromise constitutes a reason for placing a certificate on the Certificate Revocation List.
DAF	Digital application facility	
	Directory service	The directory service is a service of the UZI register which is intended to make issued certificates available and accessible on the Internet.
	End user	See certificate holder

Abbreviation	Term	Definition
	Electronic signature	A signature that consists of electronic details attached to, or logically associated with, other electronic details and which are used as a means of authentication. The electronic signature that can be placed with the UZI card is formally referred to as the 'advanced electronic signature'. This is an electronic signature that has the same legal force as a handwritten signature on paper, provided it fulfils the following requirements: - It is linked uniquely to the signatory; - It makes it possible to identify the signatory; - It is created using resources that the signatory can keep under their exclusive control; - It is linked to the electronic file in such a way that any later change to the details can be traced; - It is based on a qualified certificate as referred to in Article 1.1, section ss of the Telecommunications Act; It has been generated using a safe resource for generating electronic signatures, as referred to in Article 1.1 section vv of the Telecommunications Act.
	Electronic identity	A unique electronic representation of an identity, for example in the form of a X.500 Distinguished Name structure. These electronic details are added to or linked in a logical way with other electronic details. They act as a unique characteristic of the owner's identity.
	Escrow (Key Escrow)	'Key guarantee'. A method for storing a copy of a private key which is given to a trusted third party to keep, referred to as a 'Key Escrow Agency' (KEA).
ETSI	European Telecommunication Standard Institute	The ETSI is an independent institute in the field of telecommunications standardisation.
	Birth name	The birth name is the name included in the identity document (also known as maiden name or family name).
	Qualified certificate	A certificate that fulfils the requirements imposed pursuant to Article 18.15, second paragraph of the Telecommunications Act, and has been issued by a certificate service provider that fulfils the requirements imposed pursuant to Article 18.15, first paragraph of the Telecommunications Act.
	Authorised applicant	A care provider [zorgverlener] or representative of a (care) institution who has been authorised by the legal representative of the (care) institution to submit applications for the issue of UZI cards to the UZI register in the name of the (care) institution.
	Signature certificate (non-repudiation certificate)	A certificate that is linked to the key which must be used when placing an electronic signature.
HSM	Hardware Security Module	A resource that contains the private key(s) of systems, protects this/these key(s) against compromise and executes electronic signature, authentication or decryption on behalf of the system.
	Hierarchy	A chain of authority of mutually trusting Certification Authorities (CA).
	Identification	The process whereby the identity of a person or an organisation is established.
	Proof of identity or identity document	A document as referred to in the Compulsory Identification Act (WID) used to establish the identity of a natural person.
	Indication body	The CIZ, referred to in Article 7.1.1, first paragraph, of the Long-Term Care Act.
	Institution	A legal identity which provides care commercially, an organisational group of natural persons that provide care commercially or have it provided, as well as a natural person that has care provided commercially and the institutions designated by the Minister of Health, Welfare and Sport.

Abbreviation	Term	Definition
	Integrity	The certainty that details are complete and unchanged.
ISO	International Organization for Standardization.	Organisation that issues a number of standards and guidelines for quality management systems orientated around the quality of the main process of an organisation. The ISO standards and guidelines are internationally accepted and are revised every five years.
	Revocation code	Code with which the certificate holder can submit and authorise a revocation request for an UZI card, for example after the card has been lost.
	Irreversibility - *non-repudiation*	Irreversibility proves the origin or the receipt of details so that neither of the parties (receiver and sender) can deny the transaction or the message. In the practice of the UZI register this characteristic is linked to the certificate for the electronic signature. See also: signature certificate.
	Card applicant	The legal representative or the person for whom the legal representative has issued a financial authorisation to the UZI register in order to apply for UZI certificates.
	Cardholder	The natural person that uses the UZI card. (see also certificate holder)
PIN	Personal Identification Number	Data which is necessary in order to be able to use the UZI card. This data is personalised and must be kept secret at all times. The UZI register uses a PIN as activation data.
PUK	Personal Unblocking Key	The PUK code is needed to unblock the UZI card.
	Private key	See 'Private key'.
	PIN mailer PIN letter	The PIN letter contains the pin, puk and revocation code and, depending on the card type, is sent to the applicant or the certificate holder. The codes are printed in a secured manner so that only the party that opens the envelop knows the codes.
	PKCS#10 request	This is a file format standardised by RSA laboratories (syntax) which can be used to submit the necessary information (public key, subject information) to a CA system with which this CA system can generate a certificate. For system certificates, applicants submit a PKCS#10 request in ASCII format directly via the web registration.
PA	Policy Authority	Authority under the responsibility of the Minister of the Interior and Kingdom Relations which determines the certification policy (CP/Certificate Policy) of the UZI register. see also http://www.logius.nl
	Private key	The key of an asymmetric key pair which only has to be known to its holder and must be kept strictly secret. Sometimes the terms secret or personal key are used. See also: 'asymmetric key pair' and 'public key'.
PKI	Public Key Infrastructure	A combination of architecture, technology, organisation, procedures and rules based on asymmetric key pairs. The purpose is to facilitate reliable electronic communication and reliable electronic services.
	Public key	The key of an asymmetric key pair which can be made public. Sometimes the term public key is used. See also: 'asymmetric key pair' and 'personal key'.
RA	Registration Authority	The part of the UZI register that carries out the registration work in order to process the certificate applications.

Abbreviation	Term	Definition
	- *registration authority*	
	Revocation	Revocation concerns making a certificate invalid (withdrawal). A certificate is revoked by placing the serial number of the certificate on the Certificate Revocation List (CRL) (revocation = rescind/withdraw).
	Root CA	The highest point of trust in the hierarchy of a Public Key Infrastructure (PKI).
SSCD	Secure Signature Creation Device	A resource for generating electronic signatures that fulfils the requirements imposed in Article 18.17, first paragraph of the Telecommunications Act.
SUD	Secure User Device	A resource that contains the private key(s) of users, protects this/these key(s) against compromise and executes electronic signature, authentication or decryption in the user's name.
	Server certificate	Besides the UZI card in the form of a smart card the UZI register also issues server certificates. These server certificates can be used to demonstrate that a service (e.g. a, application or server) actually belongs to a specific care provider [zorgverlener]. In addition, a server certificate can be used to create a secure connection between services.
	Key(s)	See respectively: - Asymmetric key pair - Private key - Public key
	Key pair	See also asymmetric key pair.
	Smart card	A small plastic card the size of a credit card which contains an electronic chip, including a microprocessor, memory space and a power source. The cards can be used to store information and are easy to carry around.
	Master certificate	This is the certificate belonging to the place where the trust in all PKI for the government issued certificates originated. There is no higher CA from which the trust is derived. This certificate is signed by the holder, the party responsible for policy at the highest point of trust. All underlying certificates are issued by the holder of the master certificate.
	Assessment register	A register recognised by the party responsible for policy of the UZI register. The UZI register can issue the care provider [zorgverlener] or institution guarantee for a care provider [zorgverlener] or institution that is included in such a register.
TSP	Trusted Service Provider *provider of a certification service*	A natural person or legal identity that issues the certificates and/or provides other services connected to the electronic signatures, including identity and confidentiality. The UZI register is a TSP.
UZI	Unique Care Providers Identification	Unique way of identifying care providers [zorgverleners].
	UZI card	The bearer of the electronic identity of a care provider [zorgverlener].
	The UZI register	Register of care providers [zorgverleners]. The UZI register ensures the unique identification of care providers [zorgverleners]. It is based on a PKI which links the legal and physical identity to an electronic identity and records this in certificates. See also: www.uzi-register.nl
	Responsible party	In the context of the care institutions registration process, the responsible party means the party that is permitted to register the care institution in the UZI register.

Abbreviation	Term	Definition
	Confidentiality	The guarantee that details are exclusively available to the party to whom they are intended, without anybody else being able to decipher them. Outside the private sector, the term exclusivity is also used.
	Confidentiality certificate	A certificate that belongs with the key pair that has to be used in confidentiality applications.
	Trusting party	The natural person or legal identity that is the recipient of a certificate and acts in trust on the basis of that certificate.
Wet aanvullende Bepalingen verwerking Persoonsgegevens in de Zorg	Use of Citizen Service Number in Healthcare Act [Act Additional provisions for the processing of personal data in the care	The Use of Citizen Service Number in Healthcare Act regulates that the citizens service number is used in the care sector. The citizen service number has to be used in the care sector in order to determine unequivocally which details belong with which client.
WID	Compulsory Identification Act [Wet op de identificatieplicht]	The Compulsory Identification Act refers to the passport and identity card as a valid means of identification. A number of documents are regarded as equivalent to the passport and identity card, namely a driving licence, diplomatic passport, service or official passport, travel document for refugees or foreign nationals and other travel documents stipulated by the Minister, such as the Dutch identity card. The emergency passport and the laissez passer are not valid means of identification.
Wkkgz	Healthcare Quality, Complaints and Disputes Act [Wet Kwaliteit, klachten en geschillen zorg]	The Healthcare Quality, Complaints and Disputes Act (Wkkgz), which regulates quality and the right to complain for clients in the care sector, has been valid since 1 January 2016. The Healthcare Quality, Complaints and Disputes Act applies to all care providers [zorgverleners], including care institutions and independent professionals, such as independent entrepreneurs.
Wtza	Care Institutions (Accreditation) Act [Wet toetreding zorgaanbieders]	Care institutions need accreditation if they want to offer care which is eligible for reimbursement on the grounds of the Health Insurance Act [Zorgverzekeringswet] or Long-Term Care Act. The main purpose of entry rules is to improve the quality of care. The Care Institutions (Accreditation) Act (Wtza) regulates these accreditations.
	Legal representative	The person who, in accordance with the excerpt from the Chamber of Commerce or document of establishment, is authorised to bind the organisation legally to the UZI register.
X.509	X.509	This is an electronic certificate that is compiled in accordance with a standardised structure.
	Care	care: 1 °. care or service as described under or pursuant to the Healthcare Insurance Act and the Long-term Care Act; 2 °. form of assistance for the costs of which a subsidy is provided on the grounds of Article 3.3.3 of the Long-term Care Act or Article 68 of the Healthcare Insurance Act; 3 °. care as referred to in articles 5, 6b and 12a of the Public Health Act; 4 °. actions in the field of individual health care as referred to in Article 1 of the Individual Health Care Professions Act; all this including the financial settlement;

Abbreviation	Term	Definition
	Care providers	Care provider as referred to in the Healthcare Quality, Complaints and Disputes Act. The Healthcare Quality, Complaints and Disputes Act stipulates that a *care provider* is an institution or a care provider [zorgverlener] working alone.
	Care provider [zorgverlener]	a natural person who provides care on a commercial basis

Annex 2: Assessment criteria for organisations and care providers [zorgverleners]

The UZI register guarantees that only parties that belong to the domain indicated by the Minister of Health, Welfare and Sport can become a subscriber to the UZI register. The UZI register has two types of subscribers, namely organisations (care institutions and indication bodies) and people (care provider [zorgverlener] working alone). Both types of subscribers can apply for UZI cards for care providers [zorgverleners], other employees and services. For care provider cards [zorgverlenerpassen] the UZI register guarantees that these are issued to a care provider [zorgverlener]. If the care provider [zorgverlener] no longer fulfils the assessment criteria, the UZI register will retract the care provider card [zorgverlenerpas].

This annex clarifies the criteria on the basis of which the guarantees referred to are issued.

A. Assessment criteria for organisations
Organisations which belong to the domain of the UZI register are:
- Care providers that fall under the Use of the Act Additional provisions for the processing of personal data in the care. For the term care provider please refer to the Healthcare Quality, Complaints and Disputes Act.
- Indication body: the CIZ, referred to in Article 7.1.1, first paragraph, of the Long-Term Care Act;
- Organisations which comply with the Decree on the use of the Citizen Service Number in Healthcare, Article 2, paragraph 2 and 4.

Before an organisation is registered as a subscriber, the UZI register assesses whether the organisation belongs to the domain. In this case the following criteria are applied:
- Organisations that provide care on the basis of a law adopted by the House of Representatives and the Senate belong to the domain. These organisations do not have to submit any additional proof.
- Organisations that have an accreditation within the meaning of the Care Institutions (Accreditation) Act (Wtza) belong to the domain. These organisations do not have to submit any additional proof.
- Organisations which are included in the Pharmacies Register within the framework of the Medicines Act belong to the domain.

These organisations do not have to submit any additional proof.

If the organisation does not fall under the aforementioned categories, the organisation must submit proof. This proof can be submitted in the form of:
-
  - A copy of a document of establishment or notarial deed:
    On the basis of its objective as described in the document of establishment or the notarial deed, the organisation can demonstrate that it belongs to the aforementioned domain.
  - A copy of a licence or decision:
    On the basis of a granted licence or decision in favour, the organisation can demonstrate that it belongs to the aforementioned domain.
  - Individual declaration:
    A partnership of care providers [zorgverleners] without legal personality can be registered in the UZI register on the basis of a personal statement signed by all parties involved. This personal statement must provide evidence of a

care provider within the meaning of the Healthcare Quality, Complaints and Disputes Act.
Care agreement with a care insurer: The care provider can use this to demonstrate that this care is provided within the meaning of the Wkkgz. This statement must be signed by the legal representative and by at least 1 care provider.

B. Assessment criteria for care providers [zorgverleners]
People who are designated in the UZI register as a care provider [zorgverlener] (subscriber or certificate holder):

- Professionals as referred to in Article 3 of the Individual Healthcare Professions Act
- Professionals as referred to in Article 34 of the Individual Healthcare Professions Act.
- Professionals as referred to in Article 36a of the Individual Healthcare Professions Act.

Only healthcare providers who work solo under the Wkkgz and exercise a profession under section 3, 34 or 36a of the BIG Act can be registered as a subscriber healthcare provider in the UZI register.

You will find which professions fall under Articles 3, 34 and 36a of the BIG Act in the overview of legally protected titles.

Professional who provide care within the meaning of the Additional Provisions for the processing of personal data in healthcare, but who are not professionals as referred to in Article 3, 34 or 36a of the Individual Healthcare Professions Act.
Before a care provider [zorgverlener] is registered as a subscriber or certificate holder, the UZI register assesses whether the assessment criteria have been fulfilled. The following criteria are applied:

- The UZI register assesses whether the professional is registered in the BIG register and whether there is a situation in which the professional is not allowed to use the stated professional title or specialism (see C Criteria registration and revocation card in the event of suspension). This assessment includes any stated specialism. If the professional is registered in the BIG register and is permitted to use the professional title, the professional can be registered in the UZI register as a subscriber or holder of a care provider card [zorgverlenerpas].
  Professional groups that are subject to this assessment are:
  Pharmacists
  Doctors[22]
  Physiotherapists
  Healthcare psychologists
  Psychotherapists
  Dentists
  Midwives
  Nurses
  Physician assistant
  Orthopedagogue generalist
  Clinical technologist (Article 36a of the Individual Healthcare Professions Act)
  Registered - Dental hygienist (Article 36a of the Individual Healthcare Professions Act) [as of 1 july 2020]

22 The dispensing GP [apotheekhoudend huisarts] specialism is included in the certificates after a check has been carried out in the BIG register that the professional is allowed to invite the GP specialism and after the certificate holder has submitted a copy of the pharmacy licence.

- Professionals who are included in the Paramedics Quality Register do not have to submit additional types of proof. The UZI register assesses with the Paramedics Quality Register Foundation whether the professional is actually registered. Professional groups that are subject to this assessment are:
  Dieticians [diëtisten]
  Occupational therapists [ergotherapeuten]
  Dermatologists [huidtherapeuten]
  Speech therapists [logopedisten]
  Oral hygienists [mondhygiënisten]
  Cesar remedial therapists [oefentherapeuten Cesar]
  Mensendieck remedial therapists [oefentherapeuten Mensendieck]
  Optometrists [optometristen]
  Orthoptists [orthoptisten]
  Podiatrists [podotherapeuten]
  Radio diagnostic laboratory technicians [radiodiagnostisch laboranten]
  Radio therapeutic technicians [radiotherapeutisch laboranten]
- Professionals who are included in the Oral Hygienists Quality Register do not have to submit additional types of proof. The UZI register assesses with the Oral Hygienists Quality Register whether the professional is actually registered. Professional groups that are subject to this assessment are:
  Oral hygienists [mondhygiënisten]

- Professionals who are included in the Pharmacy assistants Quality Register (KAA) do not have to submit any additional proof. The UZI register assesses with these registers whether the professional is actually registered. The professional groups that are subject to this assessment are:
  Pharmacy assistants [apothekersassistenten][23]

- Professionals as referred to in Article 34 of the Individual Healthcare Professions Act who are not included in the Paramedics Quality Register, the Oral Hygienists Quality Register, the Pharmacy assistants Quality Register (KAA) must submit an original and validly authenticated copy of the diploma in question, or a digital excerpt thereof (pdf with certificate from DUO) with their application to be registered as a subscriber or with the application for a care provider card [zorgverlenerpas]. The UZI register decides on the basis of an assessment of the diplomas as to whether the party in question can be registered as a subscriber or holder of a care provider card [zorgverlenerpas]. Professional groups that are subject to this assessment are:

  Pharmacy assistants [apothekersassistenten][23]
  Dieticians [diëtisten]
  Occupational therapists [ergotherapeuten]
  Dermatologists [huidtherapeuten]
  Speech therapists [logopedisten]
  Oral hygienists [mondhygiënisten]
  Cesar remedial therapists [oefentherapeuten Cesar]
  Mensendieck remedial therapists [oefentherapeuten Mensendieck]
  Optometrists [optometristen]
  Orthoptists [orthoptisten]
  Podiatrists [podotherapeuten]
  Radio diagnostic laboratory technicians [radiodiagnostisch laboranten]
  Radio therapeutic technicians [radiotherapeutisch laboranten]
  Dental prosthetists [Tandprothetici]

23 This professional group cannot be regarded as a solo care provider and therefore cannot be registered as a care provider subscriber.

Individual healthcare carers [Verzorgenden in de individuele gezondheidszorg] (VIG-ers)

- Professional practitioner who provides care within the meaning of the Additional Provisions Act on the processing of personal data in healthcare, but is not a professional as referred to in Article 3, 34 or 36a of the Individual Healthcare Professions Act, must submit documents as a subscriber with their application for registration. These documents are:
    - An original certified copy of the relevant diploma or digital extract (pdf with DUO certificate)
    - A care agreement in the name of the healthcare provider (if the healthcare provide is in possession of a care agreement)
    - Declaration showing which cars is provided by the healthcare provider.

The UZI register decides on the basis of the above documents or the healthcare provider can be registered as a subscriber.

C. Consequences of a restriction on authority
The UZI register can only issue the care provider [zorgverlener] guarantee in the case of a care provider [zorgverlener] who is entitled to use the protected professional title or qualification title. In the case of the professionals in accordance with Article 3 of the Individual Healthcare Professions Act, a registration in the BIG register is an initial requirement for being eligible for the care provider [zorgverlener] guarantee. In some instances an authority restriction may apply. With regard to the authority to use the professional title in relation to the registration in the BIG register, the following situations are possible:

1 The care provider [zorgverlener] is registered in the BIG register and is fully authorised. In some instances a conditional measure may apply. Due to its conditional character, this measure will not affect the authority.
2 The care provider [zorgverlener] is registered in the BIG register and is partially unauthorised. This means that certain activities cannot be performed. The care provider [zorgverlener] can still use the professional title.
3 The care provider [zorgverlener] is registered in the BIG register and is temporarily unauthorised (this is the case in the event of a suspension or injunction). At the time of the suspension the care provider [zorgverlener] is not allowed to use the professional title and will have lost any corresponding rights.
4 The care provider [zorgverlener] has been deleted from the BIG register. The care provider [zorgverlener] is unauthorised.

Because registration in the BIG register is a requirement to be eligible for the care provider [zorgverlener] guarantee, the outlined situations can be translated as follows to the UZI register:

1 If a care provider [zorgverlener] is fully authorised, the UZI register can simply issue the care provider [zorgverlener] guarantee.
2 If a care provider [zorgverlener] is only partially unauthorised, the care provider [zorgverlener] can continue to use the professional title. The UZI register will then, in principle, issue the care provider [zorgverlener] guarantee. If the partial disqualification ought to have consequences for the care provider [zorgverlener] guarantee in the UZI card, this should be stated in the disciplinary legal judgement.
3 Although, in the event of a suspension or injunction, situations are imaginable which might be reversed on appeal, the care provider [zorgverlener] will be unauthorised at time of the suspension or injunction. Consequently, the UZI register cannot issue the care provider [zorgverlener] guarantee.

4 If the care provider's [zorgverlener] registration is deleted, the UZI register cannot issue the care provider [zorgverlener] guarantee.

Relationship between UZI card and authority

The degree of authority can be translated as being able to obtain or retain an UZI card with a care provider [zorgverlener] guarantee. Column (I) of the following table indicates what the consequences are of a card application. Column (II) indicates what the consequences are if the care provider [zorgverlener] already has a care provider card [zorgverlenerpas].

Table 16 Relationship between UZI card and authority

Authorised?	(I) UZI card application	(II) UZI card owned
Fully authorised	allocate card	no action
Partially unauthorised	allocate card	no action
Temporarily unauthorised	reject application	withdraw UZI card
Unauthorised	reject application	withdraw UZI card

Thanks to the outlined activities and method, the care sector and all trusting parties can assume that the holder of a care provider card [zorgverlenerpas] is actually a care provider [zorgverlener] as well.

Relationship between subscriber and authority

A subscriber can apply for cards for care providers [zorgverleners], employees (auxiliary staff) and systems. The relationship to the subscriber is included in these cards. For subscribers it also applies that the UZI register issues the care provider [zorgverlener] guarantee. This means that a care provider [zorgverlener] who is (temporarily) unauthorised, cannot be a subscriber to the UZI register.

If the care provider [zorgverlener] is already a subscriber, all cards issued for that subscriber will be withdrawn. This means that any cards for other care providers [zorgverleners] under the subscriber will also be withdrawn. In the event of a temporary suspension the subscriber can re-apply for cards after the suspension.

The table below shows an overview of the consequences.

Table 17 Relationship between the subscriber and authority

Authorised?	Application registration subscriber	Existing subscriber
Fully authorised	grant subscriber application	no action
Partially unauthorised	grant subscriber application	no action
Temporarily unauthorised	reject subscriber application	withdraw all subscriber's cards
Unauthorised	reject subscriber application	withdraw all subscriber's cards

In the event of a suspension or an injunction, an appeal will usually be made. In that case there is a chance that the temporary lack of authority will be designated as unjustified. In that situation consideration can be given to issuing new cards at no cost to the subscriber.

In the event of unconditional suspension of a care provider [zorgverlener] that is a subscriber, a transition period of three months will come into effect. This transition period implies the following:

- all named cards (care provider card [zorgverlenerpas] and named employee cards [medewerkerpassen op naam]) will be withdrawn in accordance with the applicable rules.
- Unnamed employee cards [medewerkerpassen niet op naam] and Server Certificates will continue to be active.

- the subscriber registration will remain active.
- no new UZI certificates may be issued under this subscriber.

After the transition period, unnamed employee cards [medewerkerpassen niet op naam] and Server Certificates will be withdrawn and the subscriber registration deleted. The UZI register does not issue any refund for any remaining period of validity of the UZI certificates.

D. Transition period 'becoming obsolete specialism'
The care provider card [zorgverlenerpas] always includes a legally protected professional title or legally protected qualification title. If applicable, the care provider card [zorgverlenerpas] also contains the legally protected specialism of the care provider [zorgverlener]. A specialism can only be included in the care provider card [zorgverlenerpas] if it is registered in the BIG register. If a specialism is removed from the BIG register, any care provider card [zorgverlenerpas] on which this specialism is stated must be withdrawn. This card may no longer be used.
The care provider [zorgverlener] in question can, of course, apply for a new UZI card without specialism or with a different specialism, recorded in the BIG register.
The UZI register assesses periodically with the BIG register as to whether the registrations of professional titles and specialisms are still up-to-date. On the basis of the outcome of this assessment the UZI register takes suitable measures. Where necessary the UZI register takes the initiative to withdraw cards.

The UZI register makes an exception to this policy if a specialism becomes obsolete This is a specialism for which no re-registration can take place. The registration of a new specialism sometimes takes place after the old specialism has been deregistered. In those instances it is impossible for the care provider [zorgverlener] to apply for a new UZI card with the correct specialism on time.

The UZI register will only withdraw the card one calendar month after it receives notification that the specialism has been removed from the BIG register. The UZI register informs the subscriber to this effect and advises the subscriber and care provider [zorgverlener] to use the month to ensure that any new specialism is registered in the BIG register and to submit a new card application.

Specialisms for which this method applies:
- neurological and psychiatric disorders

Annex 3: Professional titles, qualification titles and specialisms

The annex contains the professional titles, qualification titles and specialisms and the corresponding codes as used by the UZI register. The codes referred to are – after assessment – included in the certificates in accordance with the description in section 7.1.5 of this CPS. Although the codes referred to are fixed codes, the exact text may differ.

Article 3 of the Individual Healthcare Professions Act
Professional groups included in the BIG register are listed in the table below.

Table 18 Professional groups included in the BIG register

Term of address	Code
Pharmacist	17
Doctor	01
Physiotherapist	04
Healthcare psychologist	25
Psychotherapist	16
Dentist	02
Midwife	03
Nurse	30
Physician assistant	81
Orthopedagogue generalist	31
Clinical technologist	82

Specialisms under Article 3 professions

Table 19 Specialisms Pharmacist

Pharmacist	Code
Hospital pharmacist	060
Public pharmacist [openbaar apotheker] (Public Pharmacy)	075

Table 20 Specialisms Doctor

Doctor	Code
Allergology	002
Anaesthesiology	003
Dispensing GP [apotheekhoudend huisarts]	004
Chemical pathology	020
Public health medicine	055
Gastroenterology	013
Medical care for the mentally handicapped	056
Medical microbiology	024
Occupational medicine	008
Cardiology	010
Cardio-thoracic surgery	011
General surgery	014
Dermato-venereology	012
Obstetrics and Gynaecology	046
General practice/family medicine	015
Internal medicine	016
Allergology (closed register)	062
A youth health care physician	070
Otolaryngology/otorhinolaryngology	018
Paediatrics	019

Doctor	Code
Medical genetics	021
Geriatrics	022
Pulmonary diseases and tuberculosis	023
Neurosurgery	025
Neurology	026
Nuclear medicine	030
Ophthalmology	031
Orthopaedics	032
Pathology	033
Plastic surgery	034
Psychiatry	035
Diagnostic radiology	039
Radiotherapy	040
Rheumatology	041
Rehabilitation	042
Geriatric medicine	047
A&E doctor [spoedeisende hulp arts]	071
Sport medicine [sportarts]	074
Urology	045
Occupational medicine	048
Neuropsychiatry	050

Table 21 Specialisms Healthcare psychologist

Healthcare psychologist	Code
Clinical neuropsychology	063
Clinical psychology	061

Table 22 Specialisms Dentist

Dentist	Code
Orthodontics	053
Oral diseases and dental surgery	054

Table 23 Specialisms Nurse

Nurse	Code
Nurse spec. acute care in somatic disorders	066
Nurse spec. chronic care in somatic disorders	068
Nurse spec. mental health care	069
Nurse spec. intensive care in somatic disorders (expired as of 1-1-2021)	067
Nurse spec. preventive care in somatic disorders (expired as of 1-1-2021)	065
Nurse Spec. somatic health care (as of 1-1-2021)	076

Article 34 of the Individual Healthcare Professions Act

Qualification titles in accordance with Article 34 of the Individual Healthcare Professions Act are listed in the table below.

Table 24 Qualification titles Article 34

Term of address	Code
Pharmacy assistant [apothekersassistent]	83
Dietician	89
Occupational therapist	90
Dermatologist	88
Clinical physicist [klinisch fysicus]	84
Speech therapist [logopedist]	91
Oral hygienist [mondhygiënist]	92

Term of address	Code
Cesar remedial therapist	94
Mensendieck remedial therapist	93
Optometrist	87
Orthoptist	95
Podiatrist [podotherapeuten]	96
Radio diagnostic laboratory technician	97
Radio therapeutic technician	98
Dental prosthetist	85
VIG-er[24]	86

Article 36a of the Individual Healthcare Professions Act
Qualification titles in accordance with Article 36a of the Individual Healthcare Professions Act are listed in the table below.

Table 25 Qualification titles Article 36a

Term of address	Code
Registered - Dental hygienist [as of 1 july 2020]	79

Other Care
Professionals who provide 'care within the meaning of the Act additional provisons processing personal data in the care (Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg).

Table 26 Other Care

Term of address	Code
Care provider other care	99

24 Individual healthcare carers [Verzorgenden in de individuele gezondheidszorg] (VIG-ers)