CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Certification Practice Statement (CPS)

ZOVAR

Version 6.6

Date 31-07-2024

StatusFinal (ZV23.02)

Colophon

Organisation	CIBG Visiting address: Rijnstraat 50 2515 XP The Hague
Service desk	PO Box 16114 2500 BC The Hague T 070 340 60 20 info@zovar.nl
Version	6.6
Number of pages	70

Contents

Revision history

Version	Date	Status	Comment
1.0	01-10-2007	Final	
2.0	01-06-2008	Final	
3.0	01-09-2015	Final	
4.0	01-06-2017	Final	
5.0	04-01-2018	Final	- The Private G1 hierarchy of the State of the Netherlands release.
5.1	10-09-2018	Final	- General Data Protection Regulation (De Algemene verordening gegevensbescherming). - Limited liability with regard to performing the identification of the certificate manager added (par 9.8). - Change regarding Time required to process a revocation request modified (par 4.9.5). - Retention periods included (par. 5.5.2). - Change procedure modified (par. 9.12).
5.2	23-11-2018	Final	- Various small changes and spelling corrections (entire CPS). - The G2 hierarchy added. - Reference to chapter 3.2.2.4. of the Baseline Requirements included. - Chapter 8 'Conformity assessment' updated.
5.3	01-06-2019	Final	- Textual changes and clarifications (entire CPS). - Right to check on compensating measures added (section 4.5.2.).
5.4	01-11-2019	Final	- The G21 hierarchy – end of life. - Reference to chapter 3.2.2.4.2, 3.2.2.4.6 and 3.2.2.4.7 of the Baseline Requirements (3.2.3).
5.5	01-12-2019	Final	- Office hours added for revocation requests (par. 4.9.5).
5.6	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. - Reference to chapter 3.2.2.4.6 changed to 3.2.2.4.18 of the Baseline Requirements.
5.7	01-05-2020	Final	- Contact details changed [phone number].
5.8	01-11-2020	Final	- Revoked certificates remain on the CRL.
6.0	28-09-2021	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.
6.1	01-03-2022	Final	- Specification retention period

			- General review
6.2	02-06-2022	Final	- Change in representations and warranties
6.3	10-08-2022	Final	- General review
6.4	01-03-2023	Final	- General Review - New name telecom agency (agentschap telecom): Dutch Authority for Digital Infrastructure (Rijksinspectie Digitale Infrastructuur (RDI)) - Removed department name from server certificates - Transitional period for an organization subscriber: procedure adjusted. - Retention period of the archive: retention period of unprocessed requests added.
6.5	29-01-2024	Final	- Par. 7.1 included reference to 'CA model pas-model certificate profile' specification. - Par. 7.1.2 subscriber number added as Permanent Identifier as of Nov. 28, 2023
6.6		Final	- General update/textual changes - Par 1.1.3 added sha256fingerprints - Par.4.5.1 and 4.5.2. added the expectations for safe and acceptable certificate usage - Par. 4.9.5 and 4.9.7 adjusted maximum time period for processing of revocation requests - Par. 9.13 Ombudsman included in complaints handling - Par. 5.5.2 Selection list changed to new version - Table 2, change in OID - Table 11, under subject - OrganizationalUnitName server certificate removed

Table 1 Version history CPS ZOVAR

Accord TSP Management
Version: 6.6
Date: 26-07-2024

1. Introduction

1.1 Overview

In order to facilitate the safe communication and consultation of confidential information in the care sector, three domains have been identified: the care consumers, the care insurers and healthcare administration offices, and the care providers. The Health insurers identification and authentication register (abbreviated to ZOVAR) is the register of health insurers 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]. ZOVAR is the certificate service provider (TSP) that issues certificates for the unique identification and authentication of care insurers and healthcare administration offices. ZOVAR issues certificates with which care insurers and healthcare administration offices can request the citizen service number (BSN) from the Sectoral Healthcare Notifications Unit [Sectorale Berichten Voorziening in de Zorg] (SBV-Z). The authenticity and confidentiality functions are combined in the ZOVAR server certificates.

1.1.1 Ca model

From 4 January 2018 ZOVAR issues server certificates under a the private Root CA G1 of PKIoverheid (Private G1). With the introduction of G1, the number of levels in the CA hierarchy is a maximum of 3.

The table below shows which sha256 fingerprints are included in the relevant CA.

Issuing CA: ZOVAR Private Server CA G1
Sha256 Fingerprint: FE54263BC96C2DFBAC5BE5F449CFF7F5B12B6255A7BBCF761BA979E5986E1598

Table 2 Sha256 fingerprint

The figure 1 below shows the CA model for the generation Private G1

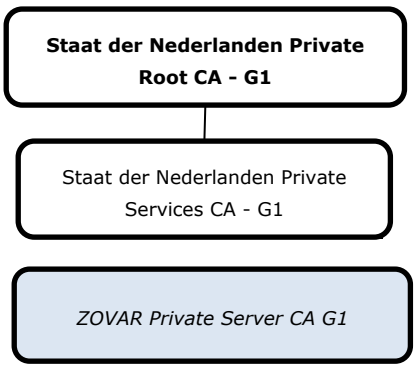

Figure 1 CA model Private Server G1

1.2 Document name and identification

1.2.1 Purpose of the CPS

The ZOVAR CPS 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. By using this CPS, the parties involved can determine their confidence in the services delivered by ZOVAR.
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 for CPSes.

1.2.2 Relationship CP and CPS

ZOVAR issues certificates within the Government domain of the hierarchy of the PKI for the government (first and second generation) and within the Organisation domain (SHA-2 generation). The requirements imposed on the issue and use of a ZOVAR certificate are described in the Programme of Requirements section 3h Certificate Policy Server Certificaten – Domein Private Services.

1.2.3 Name and references

This document is formally referred to as the 'ZOVAR 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.

CPS	Description
Naming	Certification Practice Statement, ZOVAR vX.x
Link	https://www.zorgcsp.nl/cps/zovar.html
Object Identifier (OID)	2.16.528.1.1007.15.1.1

Table 3 References to CPS ZOVAR

1.3 PKI Participants

The following parties are involved in the ZOVAR:

- implementing ZOVAR organisation, including suppliers of products and services;
- user community consists of:
  - subscribers;
  - certificate holders;
  - trusting parties.

The CIBG fulfils the role of TSP and has the final responsibility for delivering 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 'ZOVAR'.

Clauses about liability and guarantees of the TSP are included in sections9.6, 9.7 and 9.8.

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. After revocation, the CA publishes certificate serial numbers on the CRLs. Certificates are published on a CRL after the CA has received a message of revocation of the certificate from an authorised person. The CIBG has outsourced the role of CA to 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 and publish the certificates. CIBG fulfils the role of RA. CIBG has outsourced the process of establishing the identity of the certificate holder of a server certificate to KPN B.V. AMP Groep establishes the identity of the applicant/certificate manager on behalf of KPN B.V.

1.3.3 Subscribers

The subscriber is the party on whose behalf the certificate holder (i.c. server/service) acts when using the certificate. A ZOVAR subscriber is a healthcare insurer or healthcare administration office.

A healthcare insurer means:

Wlz implementing body as referred to in Article 1.1.1 of the Long-Term Care Act [Wet langdurige zorg] (Wlz);
healthcare insurer as referred to in Article 1 under b of the Healthcare Insurance Act [Zorgverzekeringswet];
insurance company as referred to in the Solvency II Directive insofar as this company offers or implements insurance policies pursuant to which the insured risk is the need for care to which, by virtue of or pursuant to the Long-Term Care Act, no entitlement exists and whereby the insured performance exceeds that arranged by virtue of or pursuant to the Healthcare Insurance Act;

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.

1.3.4 Relying parties

A relying party is the party that acts on a certificate in trust.

The obligations which are applicable to relying parties are included in sections 4.5.2 and 9.6.4.

1.3.5 Other participants

Other participants are the certificate holders and certificate managers. The applicant of a server certificate authorised on behalf of the healthcare insurer or healthcare administration office also fulfils the role of certificate manager. A certificate manager is a natural person that carries out activities on behalf of the subscriber relating to the certificate of the certificate holder. The subscriber instructs the certificate manager to carry out the activities in question and records these as proof of certificate management. As TSP the

CIBG guarantees the relationship to the subscriber and issues the server certificate after a face-to-face check and a check of the legal identity of the applicant/certificate manager. In the case of server certificates, the authenticity and confidentiality certificate are combined into a single certificate.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The field of application of certificates issued by ZOVAR is limited to the user community as described in section 1.3, section 3h of the Programme of Requirements of the PKI for the government.

ZOVAR issues server certificates. The function of an authenticity certificate and a confidentiality certificate are combined in these certificates. These functions are clarified in more detail in Table 3: Field of application of server certificate.

Application	Purpose
Authenticity and Confidentiality	This certificate is used to protect communication between machines

Table 4 Field of application of server certificate

1.4.2 Prohibited certificate uses

Certificates are issued for the purpose indicated. Otherwise there are no restrictions on the use of the certificates.

1.4.3 Test certficates

ZOVAR does not issue test products to third parties on the production environment. For own production chain tests, ZOVAR does create test certificates. These test products include 'TEST' in the organization name.

1.5 Policy Administration

1.5.1 Organization administering the document

CIBG administers the document.

1.5.2 Contact person

Information about this CPS or the services of ZOVAR can be obtained via the following contact details. Comments on this CPS can be sent to the same address:

ZOVAR
Rijnstraat 50 PO Box 16114

2515 XP The Hague
Tel: 070 340 60 20
info@zovar.nl

2500 BC The Hague

www.zovar.nl

Suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse inappropriate conduct or any other matter related to certificates can be reports t e-mail at info@zovar.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 and is assessed by an independent auditor.

1.5.4 CPS approval procedures

The CIBG is entitled to amend or supplement the CPS. Changes apply as of the moment that the new CPS commences and is published on the website www.zovar.nl. 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 Acronyms

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

2. Publication and repository responsibilities

2.1 Repositories

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

The directory service can be accessed online and is adequately secured against manipulation. 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).

ZOVAR 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

ZOVAR publishes TSP information on www.zovar.nl. Among other things, this location offers access to the following documents and services:

- CPS,
- Consultation and advisory memoranda relating to changing the CPS,
- Trusting party conditions,
- 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 section describes how the applicant/certificate manager is identified and authenticated during the initial registration procedure and which criteria the ZOVAR imposes with regard to the names.

3.1.1 Types of names

The name of the certificate holder is included in the server certificate. This field consists of (X.500) attributes and is filled as follows:

Attribute	Server
Country (C)	'NL'
Organization (O)	Subscriber's name
OrganizationalUnit (OU)	No longer applicable as of 1-12-2022.
CommonName (CN)	System name
SerialNumber	<UZOVI number><ZOVAR number>

Table 5 Name of certificate holder (subject.DistinguishedName)

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 it 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

ZOVAR does not allow the usage of pseudonyms in the subscriber registration or certificate applications.

3.1.4 Rules for interpreting various name forms

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

- The subscriber name contains the name as used during the registration in the Trade Register of the Chamber of Commerce.
- Department contains the department name given by the subscriber. This is not verified by ZOVAR.
- System name contains, for example, the fully qualified domain name (fqdn) of the system.

All names are, in principle, taken literally from the identification documents 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). If the name contains characters which are not part of this character set, ZOVAR will carry out a transition.

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

3.1.5 Uniqueness of names

ZOVAR 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 using the ZOVAR number that is included in the subject.serialNumber, preceded by the UZOVI number.

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 a healthcare insurer or healthcare administration office as referred to in the certified excerpt from the Trade Register of the Chamber of Commerce will be adopted upon registration and used in the certificates.

Applicants/certificate managers of certificates bear full responsibility for any legal consequences of using the name they provide. In the event that brand names are used the ZOVAR 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. ZOVAR reserves the right to reject the application or change the requested name if it could be contrary to trademark law.

3.2 Initial identity validation

3.2.1 Method to proof possession of private key

The key pairs are generated by the certificate manager of the subscriber. 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 a subscriber, the following must be submitted:

- A completed application form signed by the legal representative of the registration containing
    - the full name of the organisation;
    - the address 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 organisation;
    - the full name and contact details of the employee or employees who are allowed to apply for and withdraw certificates on behalf of the organisation (the authorised applicant);
    - the UZOVI number.
- 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 stated in full on the identification document. ZOVAR registers the first names, prefixes birth name, birth name and BSN from the identification document and will archive the copy of the identification document.

- Proof that the name of the organization is up-to-date and correct. This proof can take the form of:
    - the registration number under which the organization 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 organization is listed in the Trade Register of the Chamber of Commerce and which shows who is authorised to represent the organization;
    - If the organization is not registered with the Chamber of Commerce, a copy of the appointment of the legal representative can be submitted.

Organisations that have a licence granted by the Dutch Central Bank [Nederlandsche Bank] belong to the ZOVAR domain. These organisations do not have to submit any proof.
ZOVAR checks the submitted documents and details for authenticity, completeness and accuracy. ZOVAR checks whether a stated UZOVI number corresponds to the UZOVI number in the Vektis registration. ZOVAR informs the subscriber of the success 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 individual identity is authenticated upon establishment of identity within the framework of the issue of a server certificate.

A certificates application must be made by (an authorised applicant on behalf of) the subscriber that also fulfils the role of certificate manager. The following must also be submitted:

- A completed application form signed by the subscriber's applicant/certificate manager containing
    - the name of the subscriber;
    - the subscriber number;
    - the name of the applicant/certificate manager of the subscriber;
    - the name of the system or the server for which certificates are being applied.
- 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, ZOVAR checks if the subscriber can use the domain name The methods used by ZOVAR are described in chapter 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 (CSR). PKCS#10 is the common standard for a certificate request and contains the public key that is included in the ZOVAR server certificate. The PKCS#10 file must be uploaded into the application form are added to the application.

In all cases ZOVAR checks the authenticity, completeness and accuracy of the submitted documents. ZOVAR checks, on the basis of the submitted documents, whether the applicant is actually authorised to apply for the certificates. In the case of the recognised registers (Foundation for Internet Domain Registration in the Netherlands [Stichting Internet Domeinregistratie

Nederland] (SIDN) or Internet Assigned Numbers Authority (IANA)) ZOVAR checks to determine whether the subscriber owns the domain name. ZOVAR informs the subscriber of the issue of a certificate or the rejection of the certificate application. If the certificate application is rejected, the reason for the rejection will be stated.

3.2.4 Non-verified subscriber information

ZOVAR verifies the name of the subscriber on the basis of recognised documents (see sections 3.2.2 and 3.2.3).

ZOVAR verifies all details included in the certificate, with the exception of the optional 'department' field. The 'department' field optionally contains the department name given by the subscriber. This is not verified by ZOVAR. Details which are only recorded for correspondence purposes, such as correspondence name, academic titles and telephone numbers are not verified. ZOVAR adopts details which are not verified from the application form signed by an authorised applicant on behalf of the subscriber.

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. ZOVAR checks the authenticity of this application by the legal representative. ZOVAR archives this proof.

Only a legal representative can indicate who may apply for certificates on behalf of the subscriber. The method used to authenticate the legal representative is described in section 3.2.2. In the event of a server certificate application ZOVAR checks, on the basis of a copy of an identity document, whether the application has been signed by an authorised applicant.

3.2.6 Criteria for interoperation

No stipulation.

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.

The certificate can be renewed using a certificate renewal application form. These application forms will be submitted on time by ZOVAR together with the renewal letter. Only original certificate renewal application forms which have been sent out by ZOVAR will be processed. The renewal letter and the application form must be sent out no less than 3 months before the expiry date. 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

Keys are renewed after revocation of the certificate in accordance with an initial application. A new key pair is always generated when a renewal request is executed. See the procedure in section 3.3.1 'Routinematige vernieuwing van het certificaat'.

3.4 Identification and authentication for revocation request

The legal representative of an authorised applicant can submit revocation requests on behalf of the subscriber. Requests to withdraw certificates can be made electronically, by email or by post. It is not possible to make requests to withdraw server certificates by telephone[1].

In the event of requests for **electronic revocation** identification and authentication take place on the basis of a number and a revocation code. The number and the revocation code are sent to the subscriber in writing when the certificate is issued.

In the event of requests for revocation by **non-electronically signed email or by post**, identification and authentication will take place on the basis of a request signed by the person authorised to withdraw. ZOVAR 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, ZOVAR will carry out the revocation request.
- If the signature does not correspond, ZOVAR will telephone the subscriber using the contact details registered with the ZOVAR. The applicant will then be asked to place the signature in accordance with the WID archived with ZOVAR. If the signature on the WID is changed, the applicant will be asked to send a valid copy of the WID to ZOVAR. After another check of the signature, ZOVAR will carry out the revocation request. ZOVAR archives the new copy of the WID.

In the event of requests for revocation via **electronically signed email** the requirement will be that the email is signed by the person authorised to withdraw with a qualified non-repudiation certificate (such as on a PKI government card).

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

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 an applicant and a legal representative. These applicants are authorised by the subscriber to submit applications. Applications must always be submitted in writing. PKCS#10 files can only be sent via the website or via electronically signed mail.

4.1.2 Enrollment process and responsibilities

Cancelling an application is in principle not possible after submitting an application. Exceptions, in exceptional cases, 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 ZOVAR.

4.2 Certificate application processing

Before certificates can be applied for, the subscriber must be registered with ZOVAR. For this, the following steps have to be completed:

- The intended subscriber submits a completed and signed application form, including the documents indicated in section 3.2. The intended subscriber can fill in forms via the ZOVAR website or can request these from ZOVAR. Before completing the application form the subscriber must be familiar with all the applicable conditions in the CPS. ZOVAR will not process any incomplete applications.
- ZOVAR carries out the checks referred to in section 3.2 and informs the subscriber of the result. If ZOVAR has informed the subscriber in writing that they cannot be registered, the subscriber will have six weeks to submit an objection.

A subscriber can apply for server certificates after registration. For this, the following steps have to be completed:

- The 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 (www.zovar.nl). Before completing the application form the applicant/certificate manager must be familiar with all the applicable conditions in the CPS. ZOVAR will not process any incomplete applications.
- ZOVAR archives the submitted documents so that they can be used as proof in the event of reconstruction in accordance with current laws and regulations.

ZOVAR does not check Certification Authority Authorization DNS details on behalf of any 'certificate pinning' by the subscriber.

4.2.1 Performing identification and authentication functions

ZOVAR performs the checks as described in section 3.2 and 4.3.

4.2.2 Approval or rejection of certificate applications

ZOVAR carries out the checks referred to in section 3.2 and informs the

subscriber of the issue of the certificate or the rejection of the application. If the application is rejected, the reason for the rejection will be stated and the subscriber will have six weeks to submit an objection.

4.2.3 Time to process certificate applications

The maximum turnaround time applied by ZOVAR is no more than eight weeks from receipt of the completed application until the ZOVAR server certificate is available. ZOVAR may require more time during extremely busy periods. Information on this will be issued on the website www.zovar.nl.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

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:

- The applicant/certificate manager signs the PDF application form with a qualified non-repudiation certificate. Or;
- The applicant/certificate manager sends the ZOVAR an email containing the completed application form. The applicant/certificate manager signs this email with a qualified non-repudiation certificate.

The employee of ZOVAR 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:

- The applicant 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 applicant 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). ZOVAR is obliged to archive a copy of the document used to prove identity. The data on the copy that are not relevant to ZOVAR are shielded using automatic recognition software.
- 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 ZOVAR. AMP Groep is fully certified to do this (in accordance with ETSI EN 319411-2).
- The applicant signs the proof of identification. The applicant 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 ZOVAR, instructions will be given to produce the server certificate.If the applicant does not schedule an appointment for identity determination by AMP group, AMP group will send several reminders to come to an appointment. If the final identification period is exceeded, the application will be rejected.

4.3.2 Notification to subscriber by the CA of issuance of certificate
After a servercertificate has been produced, ZOVAR sends the certificate by email to the applicant. ZOVAR also sends a revocation code to the subscriber's correspondence address for the attention of the applicant.

4.4 Certificate acceptance

The conditions for the use of certificates of ZOVAR are stated in the CPS. The CPS is published on the website.

4.4.1 Conduct constituting certificate acceptance
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 is obliged to inform ZOVAR immediately and to withdraw the certificates if an irregularity occurs as indicated in section 4.9.1.
- The subscriber and the certificate holder are obliged to stop using the certificates and the corresponding private keys if instructed to do so by ZOVAR. ZOVAR can provide an indication like this in the event that a CA key is compromised.
- 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 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 must ensure that the key material is exclusively generated in a safe resource that complies with EAL 4+ or equivalent security criteria.
- 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 of such quality that it is practically impossible to steal or copy the keys without being noticed[2].

- The subscriber is obliged to keep the activation details, which are used to obtain access to the private key, separate from the SUD.
- If the 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 subscriber and applicant of a certificate requests confirms that ZOVAR is entitled to issue personal data, such as name, address, email and telephone number to KPN B.V.,Cannock Outsourcing B.V. and AMP Groep.
- The subscriber confirms that ZOVAR is entitled to withdraw the certificate if the subscriber violates the applicable conditions or if the ZOVAR establishes that the certificate is being used in conjunction with criminal activities, for example phishing attacks, fraud, or the distribution of malware.
- The Subscriber is responsible for prompt replacement of its certificate(s) in the event of an approaching expiry of validity, and for emergency replacement in the event of a private key compromise and/or other types of emergencies relating to the certificate or the higher level certificates.
- The Subscriber is expected to take adequate measures in order to safeguard the continuity of the use of certificates, and
- The Subscriber is expected to take into account security best practices in the usage of certificates.
- The above obligations for the subscriber will, insofar as they can be designated as too uncertain, be developed in more detail in ZOVAR guidelines and/or more detailed regulations.

4.5.2 Relying party public key and certificate usage

The obligations of the relying party are applicable when trusting a certificate issued by ZOVAR. The relying 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 the validity of the certificate by means of the most recently published Certificate Revocation List (CRL) or via the Online Certificate Status Protocol (OCSP);
- always to use the most recently published Certificate 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

2 ZOVAR has the right to check the compensating measures

by trusting parties;
- to be aware that previous checks only authenticated the integrity of the details and the identity of the server or service and did not constitute a judgement on the content of the details.

The expectations for safe and acceptable certificate usage:
- The Subscriber is responsible for prompt replacement of its certificate(s) in the event of an approaching expiry of validity, and for emergency replacement in the event of a private key compromise and/or other types of emergencies relating to the certificate or the higher level certificates,
- The Subscriber is expected to take adequate measures in order to safeguard the continuity of the use of certificates, and
- The Subscriber is expected to take into account security best practices in the usage of certificates.

4.6 Certificate Renewal

If, after the (threatened) expiry of the period of validity or after an application for revocation, a ZOVAR-certificate 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 the revocation, new server certificates are 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 existing 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. ZOVAR ensures that date and time of revocation of certificates can be established exactly. In the event of any doubt the time determined by ZOVAR will apply as the moment of revocation. If a certificate is withdrawn, it cannot be declared valid again.

ZOVAR does not permit the (temporary) suspension of certificates.

4.9.1 Circumstances for revocation

The subscriber is obliged to submit a revocation request to ZOVAR and to terminate the use of the certificate in the following circumstances:

- observed or suspected misuse or compromise;
- termination of the subscriber's existence;
- inaccuracies in, or changes to, the details shown on the certificates;
- system/server no longer used;
- permission to use the domain name is withdrawn.

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

- All certificates of a subscriber can be withdrawn if the subscriber does not comply with the obligations in the CPS[3].
- All certificates of a subscriber are withdrawn if the Dutch Central Bank no longer designates them as a healthcare insurer or if the Ministry of Health, Welfare and Sport no longer designates them as a healthcare administration office.
- A server certificate is withdrawn if the owner of the domain name reports to ZOVAR that the permission to use the domain name has been withdrawn.
- One or more certificates of a subscriber are withdrawn if ZOVAR observes inaccuracies in the details included in the certificate, for example due to a name change.
- The certificates of a subscriber can be 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).
- A server certificate is withdrawn if the invoice is not paid for by the set deadline[4].

The reasons for each revocation initiated by ZOVAR are to be documented, archived and signed by the TSP management.

4.9.2 Who can request revocation

A request to withdraw certificates may be submitted by:

- an authorised applicant on behalf of the subscriber in the role of certificate manager;
- the legal representative of the subscriber;
- the curator that acts if the subscriber itself is no longer authorised to perform legal actions with intended legal consequence;
- In addition, ZOVAR is authorised initiate withdrawals.

A trusting party cannot make a revocation request but can report the suspicion of a circumstance which may cause the revocation of a certificate. In such an instance ZOVAR will investigate the report and will withdraw the certificate if necessary.

3 The conditions for the subscribers are included in CPS sections 4.5.1 and 9.6.2.
4 As stated in section 9.1.7, the deadline is set at six weeks after receipt of the reminder.

4.9.3 Procedure for revocation request

Requests to withdraw certificates can be made by a certificate holder, an appropriately authorised person of the subscriber, or by the certificate holder electronically, or by emailof 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 ZOVAR (www.zovar.nl). This form of revocation is available twenty-four hours per day, seven days per week.

In the event of a request for **electronic** revocation, the applicant/certificate manager fills in a number that has been communicated with the corresponding revocation code on the website (www.zorgcsp.nl). If the revocation code and smart card number are correct, the certificate 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 the revocation will not be carried out. ZOVAR has taken measures to make it impossible to make unlimited incorrect revocation requests.

In the event of requests for revocation **by non-electronically signed email or by post** the following 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 certificate or the certificates for which the request applies.

ZOVAR 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, ZOVAR will carry out the revocation request.
- If the signature does not correspond, ZOVAR will telephone the subscriber using the contact details registered with the ZOVAR. The applicant will then be asked to place the signature in accordance with the WID archived with ZOVAR. If the signature on the WID is changed, the applicant will be asked to send a valid copy of the WID to ZOVAR. After another check of the signature, ZOVAR will carry out the revocation request. ZOVAR archives the new copy of the WID.

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

- The email is signed by the person authorised to withdraw with a qualified non-repudiation certificate (as on a PKI government card).

ZOVAR checks whether the party submitting the revocation request is authorised to make the application. ZOVAR also checks the identity of the party submitting the revocation request on the basis of the submitted identity document and a previously archived copy of the identity document. After carrying out the checks ZOVAR withdraws the certificates and places them on the Certificate Revocation List (CRL). A confirmation that the revocation has been accepted, or a notification that the revocation request has been rejected, will be sent in writing to the subscriber.

4.9.4 Revocation request grace period

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

4.9.1.

4.9.5 Time within which CA must process the revocation request

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

Requests for revocation received by email, upload page, or mail will be processed within twenty-four hours if the request is received on business days before 4:00 PM. Revocation requests received by email, upload page, or mail after 4:00 PM on business days, or during weekends or holidays, will be processed on the next business 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 publische CRL of 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 issue frequency

The CRL issue frequency is every hour and the CRL is valid for 48 hours. In the event of system defects, service activities or other factors outside ZOVAR's control, ZOVAR also ensures that revocation requests which are submitted via electronic withdrawal are carried out within twenty-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 ZOVAR 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).

Withdrawn certificates will remain on the CRL, even after the original validity date had passed.

4.9.8 Maximum latency for CRLs

The CRL is published immediately after generation.

4.9.9 On-line revocation/status checking availability

In addition to the publication of CRLs, ZOVAR 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 het CA in question.

OCSP validation is an online validation method whereby ZOVAR 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 ZOVAR. 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 we do not receive an OCSP response, 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.

A 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 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 On-line revocation checking requirements
This service is freely available to all trusting parties who want to validate the revocation status of a certificate issued by ZOVAR.

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
ZOVAR does not permit the (temporary) suspension of certificates.

4.9.14 Who can request suspension
ZOVAR does not permit the (temporary) suspension of certificates.

4.9.15 Procedure for suspension request
ZOVAR does not permit the (temporary) suspension of certificates.

4.9.16 Limits on suspension period
ZOVAR does not permit the (temporary) suspension of certificates.

4.10 Certificate Status Services

4.10.1 Operational characteristics
ZOVAR 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, ZOVAR 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

No end date applies, in principle, to the subscriber registration. The registration can be terminated at the request of the subscriber or if the registered person can no longer be regarded as a care office or health insurer.

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

In the event of a name change or termination of a subscriber, a transition period will come into effect. This transition period implies the following:

- ZOVAR sends an intention to cancel the subscription, on which the subscriber has two weeks to give his or her opinion.
- Three weeks after the intention to cancel the subscriber's registration, **provided the circumstances remain unchanged,** ZOVAR takes a decision to cancel the subscriber registration:
    - The subscriber registration remains valid during the objection period (6 weeks)
    - Server certificates remain valid during the objection period (6 weeks)
    - It's not possible to apply for new server certificates.

One week after the objection period has expired the server certificates shall be revoked and the subscriber registration shall be canceled.
ZOVAR does not provide any refund for the remaining period of validity of revoked certificates.

If no server certificates are active under the subscription registration, ZOVAR will take a decision to cancel the subscriber registration immediately after the ZOVAR is notified of the event, in this case there will be no transition period.

4.12 Key escrow and recovery

ZOVAR 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 ZOVAR are provided from various locations. The registration work is carried out at CIBG's premises. The certification takes place at the computing centre of KPN Corporate Market B.V. The work in relation to the mobile identification of the certificate manager 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 protected and properly protected registration, certification, issue and revocation process which 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 the computing centre of KPN Corporate Market B.V. in Apeldoorn. This environment fulfils the law and regulations imposed by the government, including the Protection of State Secrets Act 1951 [Wet Bescherming Staatsgeheimen 1951]. 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.

ZOVAR 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 of versions, changes and emergency repairs to all operational software. Before software can be put into production, ZOVAR carries out tests on the basis of predetermined test plans.

ZOVAR 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 chapter 5.1.2.

5.1.4 Water exposures

See chapter 5.1.2.

5.1.5 Fire prevention and protection

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.

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 ZOVAR. 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 ZOVAR 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

ZOVAR 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), Chief Information Security Officer (CISO), 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 ZOVAR have the required knowledge and experience in the field of certification services. Employees who are responsible for checking identification documents have the knowledge required to check the authenticity of the documents.

Security tasks and responsibilities, including those for confidential positions, are documented in 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. Employee authorisations are granted based on the '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 certification work. ZOVAR asks all employees involved in registration and identification to submit a certificate of good conduct.

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

5.3.3 Training requirements
ZOVAR deploys sufficient personnel who have enough specialist knowledge, experience and qualifications 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 that performs an authorised 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
ZOVAR 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

ZOVAR 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.

ZOVAR 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 randomly 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
No stipulation.

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
ZOVAR carries out a more detailed investigation if the logging reveals malicious activities.

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

5.5 Records Archival

5.5.1 Types of records archived
ZOVAR archives all relevant information relating to events, details, files and forms. The following is recorded as a minimum:

- 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).
- Storage location of copies of applications and identity documents.
- Information which is relevant for the identification of a subscriber.
- Information concerning the checks carried out.
- Correspondence relating to registration application or certificate application.
- Proof of date and time of issue of the certificates.
- Information concerning revocation requests of certificates or deletion from the registration.
- Complaints and objections and correspondence received in relation to complaints objections.
- Requests for information received in writing and other correspondence related to the Personal Data Protection Act [Wet bescherming persoonsgegevens] or the Government Information (Public Access) Act [Wet open overheid].

5.5.2 Retention period for archive
All archived events are stored in accordance with process 10.33 of the selection list[5] throughout the period of validity of the qualified certificate and for a period of at least seven years after the date on which the validity of the qualified certificate expires. Applications that have not been processed will be kept for a period of one year in accordance with process 10.33 of the selection list.[6]

Alle archived events with regard to the subscription registration are stored for

6 Department-wide selection list of the Ministry of Health, Welfare and Sport (VWS)

a period of at least seven years from the date on which the subscription registration is deleted.

5.5.3 Protection of Archive
ZOVAR ensures the integrity and accessibility of the archived details. ZOVAR arranges careful and secure storage and archiving.

5.5.4 Archiving 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 of the issue of a certificate is recorded upon issue.

5.5.6 Archived collection system (internal or external)
Electronic archiving takes place at physically separated locations (online data 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 made available in the directory and on the website.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

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

In the event of any compromising of keys, or in the event of calamities, ZOVAR can instigate an investigation, but is not obliged to do so. In the event of compromise of (one of) the private key(s) of ZOVAR, ZOVAR will take the following action as a minimum:

- ZOVAR will inform trusting parties, subscribers and certificate holders as soon as possible by publishing the information on https://www.zovar.nl.
- ZOVAR will inform the subscribers in question via an email sent to the email address provided at registration.
- If such is necessary, ZOVAR will immediately withdraw the certificates in question and publish them on the applicable CRL.
- ZOVAR will immediately inform the PKI Policy Authority for the government, The Dutch Authority for Digital Infrastructure (RDI), NCSC, certifying authority and optionally Dutch Data Protection Authority (AP) in the event of a calamity.

In the event of compromise of one of the algorithms used by ZOVAR, ZOVAR will consult with the Policy Authority of the PKI for the government. In principle ZOVAR 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 Entity 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 ZOVAR terminates the certification services, this will be done in accordance with a controlled process as described in more detail in the ZOVAR 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

6.1.1 Key pair generation

When generating key pairs, ZOVAR uses reliable procedures in a secure environment which complies with objective and internationally recognised standards. The keys of the CAs of ZOVAR were generated in a FIPS 140-2 level 3 certified Hardware Security Module (HSM). The keys of the CAs are 4096 bit RSA. This involves the use of the 'SHA256RSA'.
In the case of user certificates, the subscriber will submit the public key to the RA via a Public Key Certificate Signing request (PKCS#10).

6.1.2 Private key delivery to subscriber

The private key is not transferred. The certificate and the certified public key are sent to an email address provided upon application after the certificate manager on behalf of the subscriber has appeared in person.

6.1.3 Public key delivery to certificate issuer

In the case of server certificates, the key pair is generated by the subscriber. The public keys are sent via secured connections in signed messages to the CA for signing.

6.1.4 CA public key delivery to relying parties

The public key of the ZOVAR CA has been signed by the Domain CA of the Policy Authority, as a result of which the integrity and origin of the public key is safeguarded. These public keys are made available to trusting parties in the form of CA certificates, via www.zovar.nl.

The State of the Netherlands Private root CA –G1 certificate, the State of the Netherlands Government CA – G1 certificate and the ZOVAR Private Server CA – G1 certificate are available via https://cert.pkioverheid.nl/.

6.1.5 Key sizes

The key length in a server certificate is at least 2048 bit RSA. The key length in a CA-certificate is 4096 bits RSA.

6.1.6 Public key parameters generation and quality checking

Checking ZOVAR 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: Key Usage).

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standard 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 ZOVAR cannot be read in one go. A backup is made of the private keys of the CAs of ZOVAR. The backup is saved in cryptographic modules in several encrypted parts. The backup can only be used if several parties are present with their section of the key.

6.2.3 Private key escrow
ZOVAR does not take private keys of certificate holders in escrow.

6.2.4 Private key backup
ZOVAR does not make a backup of the private keys of certificate holders.

6.2.5 Private key archival
ZOVAR does not archive any private keys of certificate holders.

6.2.6 Private key transfer into or from a cryptographic 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 key
The private keys of the CAs of ZOVAR can only be activated by means of a key ceremony and in the presence of the necessary officials. ZOVAR ensures a careful procedure in a secured environment.

6.2.9 Method of deactivating private key
In instances to be determined by ZOVAR, the private keys will be deactivated with due regard for the applicable due diligence procedures.

6.2.10 Method of destroying private key
The private keys with which certificates can be signed, cannot be reused after the end of their life cycle. ZOVAR arranges adequate destruction to ensure that it is impossible to trace the destroyed keys from the remnants.

6.2.11 Cryptographic Module Rating
The Hardware Security Modules used within the ZOVAR 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 corruption can be detected. Each consignment is checked immediately after the arrival on the basis of the corresponding out-of-band list.

6.3 Other aspects of key pair management

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

6.3.1 Public key archival

Public keys are archived by the ZOVAR 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 6 provide an overview of the validity of the key pairs and CA certificates of the Private G1 hierarchy.

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

Table 6 validity CA Certificaten Public G3/Private G1 hiërarchie

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

ZOVAR only issues server certificates. The subscriber must take suitable measures in accordance with the obligations in section 4.5.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The registration systems of ZOVAR include suitable checks and security measures. Partly as a result of this it is impossible for a certificate application to be processed by one employee of ZOVAR.

ZOVAR 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. ZOVAR 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

ZOVAR classifies the resources used on the basis of a risk analysis.

6.6 Life cycle technical controls

6.6.1 System development controls

ZOVAR does not engage in system development itself. An independent EDP auditor has issued an audit certificate for the systems used on the basis of CWA 14167-1. ZOVAR carries out tests before the systems are put to use. Testing takes place on the basis of test plans drawn up in advance.

6.6.2 Security management controls

ZOVAR 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 of 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 which can 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.

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

The capacity usage is monitored and predictions are done of the capacity required in the future 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 ZOVAR is subject to stringent safety measures (up-to-date firewall, virus scanners, proxy).

6.8 Timestamping

No stipulation.

7. Certificate, CRL and OCSP profiles

7.1 Certificate profile

This section provides a general overview of the ZOVAR certificate profile. In particular, the fields that contain relevant data for certificate holders are discussed.

An X.509 certificate consists of a collection of 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 basic attributes and extensions are shown in the following subsections.

A more detailed technical description is available at https://www.uziregister.nl/documenten titled 'CA model pasmodel certificaat profielen'.

7.1.1 Version number(s)

The ZOVAR certificates comply with the X.509 v3 standard and also comply with Part 3h of the Programme of Requirements of the PKI for the Government, (see www.logius.nl);

7.1.2 Certificate Extensions

Basic attributes

The certificates from ZOVAR have the following basic attributes insofar as they are not described in other sections:

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

Table 7 Basic attributes of certificate profiles

Standard extensions

ZOVAR certificates contain the following standard extensions:

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.
KeyUsage	Yes	Contains the DigitalSignature and KeyEncipherment bits.
BasicConstraints	Yes	The CA bit is set to 'False' and pathLenConstraint to 'none'.

Field	Essential	Value
CertificatePolicies	No	Contains: • the Object Identifier (OID) for the applicable Certificate Policy of the PKI for the Government (see par. 7.1.6); • A link to the CPS of ZOVAR (see Table 1); • a user text (UserNotice): 'The field of application of this certificate is limited to communication within the Government domain as indicated in the Programme of Requirements of the PKI for the Government. See www.logius.nl'
AuthorityInfoAc-cess.accessMethod (OCSP)	No	This attribute includes the URL of the OCSP services: http://ocsp.zovar.nl
AuthorityInfoAc-cess.accessMethod (CA Issuers)	No	In this attribute the URL is included to CA certificate of the issuing CA: http://cert.pkioverheid.nl/ZOVAR_Private_Server_CA_G1.cer
ExtendedKeyUsage	No	ZOVAR certificates include the following ExtendedKeyUsages: - ServerAuthenticatie - ClientAuthenticatie
SubjectAltName	No	In this attribute various members are included in the subjectAltName.otherName, see clarification below. In addition to the subjectAltName.otherName, as of November 28, 2023, the subscriber number is included as a Permanent Identifier in the SubjectAltname extension.
CrlDistributionPoints	No	Contains the URI where the CRL can be retrieved: http://www.csp.zovar.nl/cdp/zovar_private_server_ca_g1.crl

Table 8 Standard extensions of certificate profiles

Clarification SubjectAltName.otherName
This section describes how the subjectAltName.othername is included in the ZOVAR certificates.

PKI government 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 '-'.

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

CA	OID
TSP CA	2.16.528.1.1003.1.3.5.5.1
ZOVAR Server CA	2.16.528.1.1003.1.3.5.5.6

Table 9 <OID CA> production environment SHA-2 generation

Values SubjectAltName.otherName: <Subject ID>

The <Subject ID> in ZOVAR is a compound field, consisting of fields separated by a '-':

<Subject ID> = <version-no.>-<subject-no.>-<card type>-<UZOVI-no.>-<recognition>

The following table clarifies the fields:

Field	Type	Value	Explanation
version no.	1NUM	1	Version number of the <Subject ID> specification for possible future developments.
subject-no.	13NUM	<UZOVI number><ZOVAR number>	A unique number for ZOVAR server certificate.
card type	1CHAR	The following coding is used: 'V' : Server certificates	
UZOVI no.	4NUM	UZOVI number	The Vektis UZOVI number
recognition	2CHAR	Type of recognition: 'ZV': Health insurer	The recognition will, in the first instance, always the filled in with 'ZV' because only care insurers can be ZOVAR subscribers

Table 10 Fields <Subject ID> in SubjectAltName.otherName

Private extensions
The ZOVAR certificate does not contain any private extensions.

7.1.3 Cryptographic algorithm object identifiers

The certificates of ZOVAR 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 ZOVAR 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 CA and is shown by the attributes OrganizationName, CommonName, organizationIdentifier and CountryName. These have the following fixed values: **OrganizationName** 'CIBG' **organizationIdentifier** 'NTRNL-50000535' **CommonName** 'ZOVAR Private Server CA G1' **CountryName** 'NL' (in accordance with ISO 3166).
Subject	The name of the subject is shown as a Distinguished Name (DN) and is shown by at least the following attributes: CountryName, CommonName, OrganizationName, StateOrProvinceName, LocalityName and SerialNumber. The

Field	Value
	attributes which are filled as follows: **CommonName** name of the system. **OrganizationName** name of the subscriber. **StateOrProvinceName** province of the subscriber. **LocalityName** place name of the subscriber. **CountryName** country of the subscriber (in accordance withISO 3166). **SerialNumber** the UZOVI number directly followed by the ZOVAR number.

Table 11 Name forms

7.1.5 Name constraints
For the names in certificates, the preconditions arising from RFC 5280 and the Programme of Requirements PKIoverheid apply.

7.1.6 Certificate policy object identifier
For the Certificate Policies (CP) reference is made to www.logius.nl. In order to be able to identify the correct CP, the table below shows the relationship between the certificates, 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.

Type of certificate		Applicable CP	OID CP
Name	**Certificate (function)**		
Server (Private G1)	authenticity and confidentiality	*PvE deel 3h: Certificate Policy Server Certificaten – Domein Private Services*	2.16.528.1.1003.1.2.8.6

Table 12 Overview of certificates with OID of applicable CP

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 ZOVAR 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 3h of the Programme of Requirements of the PKI for the government (see www.logius.nl). The profile of the CRL for the certificates contains a number of attributes and extensions. These are shown in the following subsections.

7.2.1 Version number(s)

ZOVAR issues CRLs according to the X.509 version 2 format.

7.2.2 CRL and CRL entry extensions

The CRL for certificates of ZOVAR has the following attributes:

Field	Value
Version	1 (X.509 version 2)
signatureAlgorithm	sha-256 WithRSAEncryption
Issuer	Contains the name of the CA and is shown by the attributes OrganizationName, CommonName, organizationIdentifier and CountryName. OrganizationName ‘CIBG’ organizationIdentifier ‘NTRNL-50000535’ CommonName'ZOVAR Private Server CA G1' CountryName 'NL' (in accordance with ISO 3166).
thisUpdate	Date/time of issue.
nextUpdate	This is the date/time on/at which the validity of the CRL ends. The value is 'thisUpdate' plus forty- eight hours. ZOVAR publishes an update of the CRL every hour.
revokedCertificates	The revoked certificates per entry: - certificate serial number - date/time of revocation

Table 13 CRL attributes

The CRL for ZOVAR certificates has the following extensions:

Field	**Essential**	**Value**
AuthorityKeyIdentifier	No	Contains 160 bit SHA-1 hash of the public key of the CA that signed the CRL.
CRLNumber	No	Serial number
ExpiredCertsOnCRL	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

Table 14 CRL extensions

7.3 OCSP profile

7.3.1 Version number(s)

The OCSP service of ZOVAR 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 ZOVAR certificates uses the URL http://ocsp.zovar.nl
- Each CA of ZOVAR that issues user certificates has its own OCSP responder that signs the OCSP responses with its own private key;
- 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 ZOVAR Private Server CA G1'.
- 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 ZOVAR 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 ZOVAR 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 ZOVAR were certified as per 22-11-2004 on the basis of the 'Scheme for certification of Certification Authorities against ETSI TS 102 042 and therefore fulfils the requirements imposed on certification service providers. The certification of CIBG for ETSI 102 042 (policies NCP+, OVCP and PTC-BR) has been followed up by 319 411-1 as of 1 July 2016

A copy of the EN 319 411-1 certificate can be found on the ZOVAR website (see certification policy).

As a Trust Service Provider ZOVAR is registered with the Agentschap Telecom under registration number 940473, as a verified issuer of qualified certificates to the public and is therefore a certificate service provider within the meaning of the Telecommunications Act. As of 1 January 2023, the name of agentschap Telecom has been changed to the Rijksinspectie Digitale Infrastructuur (RDI, the dutch authority for digital infrastructure).

8.1 Frequency or circumstances of assessment

The audit cycle is performed in accordance with the ETSI EN 319 403 certification schedule. ZOVAR 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 ZOVAR carries out internal audits and self-assessments itself.

8.2 Identity/qualifications of assessor

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

8.3 Assessor's relationship to assessed entity

The auditors that perform the audits are independent. Otherwise there is no additional relationship between CIBG as TSP 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 certificates permanently fulfils the requirements in the standards ETSI EN 319 411-1 (policies NCP and OVCP), and part 3h of the Programme of Requirements of PKI government.

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 CIBG 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 ZOVAR website and in the electronic storage location of the Policy Authority of the PKI for the government. The TSP services of the CIBG also comply 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 for the ZOVAR server certificate, by a healthcare insurer registered in ZOVAR (subscriber), is subject to a cost-covering rate. This rate is applicable to both the initial application and the subsequent application, including renewal, of the ZOVAR server certificate. The rates for the ZOVAR server certificate can be found on www.zovar.nl.

No cost are charged for rejected applications.

9.1.2 Certificate access fees

ZOVAR does not charge any fees for certificate access.

9.1.3 Revocation or status information access fees

ZOVAR does not charge any fees for revocation or status information access.

9.1.4 Fees for other services

No stipulation.

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 pass or certificate

9.1.6 Rate changes

The rate for the ZOVAR server certificate 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.zovar.nl.

9.1.7 Invoicing and payment

Three weeks after the production date of the ZOVAR Certificate, the subscriber will receive a related invoice at the postal address registered with ZOVAR. In addition, the invoice will be sent in digital form to the applicant's email address.

ZOVAR 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. ZOVAR will not honour a request for a modification to an invoice.

The applicant is responsible for choosing the right ZOVAR certificate. If the applicant applies for a certificate which turns out to be incorrect, for example

due to a 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, ZOVAR is entitled to instigate collection measures and/or engage a third party to collect the claim. In the event of late payment the ZOVAR certificate will be withdrawn by ZOVAR. The revocation of the ZOVAR certificate will take place six weeks after the reminder has been sent.

9.1.9 Validity of ZOVAR server 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 a ZOVAR server certificate is three years after the production date.

9.1.10 Delivery and initial usage of ZOVAR server certificate
The ZOVAR server certificate is delivered in accordance with the technical and/or functional specifications referred to in the Certification Practice Statement (CPS). The subscriber will start using the ZOVAR server certificate within three months after its receipt. If it transpires, upon initial usage, that the ZOVAR server certificate is not functioning optimally, the subscriber or its authorised representative will immediately inform the ZOVAR to this effect.

9.1.11 Replacement conditions
If the ZOVAR server certificate does not work in accordance with the technical and/or functional specifications described in the CPS, ZOVAR will replace this certificate free of charge during the first three months after transfer of the ZOVAR server certificate.

9.1.12 Risk, ownership and duty of care
The risk of destruction, loss or theft, damage or deterioration of the ZOVAR server certificate transfers to the subscriber at the moment of receipt of the ZOVAR server certificate. The subscriber is not entitled to make any changes to the ZOVAR server certificate. The issued ZOVAR server certificate will continue to be owned by ZOVAR. ZOVAR is authorised to withdraw the use of the ZOVAR-server certificate by a subscriber. ZOVAR server certificates cannot be transferred to third parties. The subscriber or its authorised representative must ensure that the ZOVAR server certificate is used and stored in a careful, safe and prudent manner.

9.2 Financial Responsibility

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 Open Government Act [Wet open overheid] anyone can make a request for public information. The application shall specify the matter or the related document on which the applicant wishes to receive information.

If ZOVAR outsources work to third parties, this work will be carried out under the responsibility of ZOVAR. The agreements between third parties and ZOVAR have been 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 ZOVAR, the purchasers of its services, or of one of the third parties engaged by ZOVAR, these will not be made available to others, except those parties that have to have 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 ZOVAR.

The certificate managers are entitled to meet and correct their personal details.

9.4.2 Information treated as private
The information obtained by ZOVAR about a person, being a natural person or legal entity, will be treated as confidential. The requirements imposed in the General data protection [Algemene verordening gegevensbescherming] (AVG) are explicitly applicable to this. The following documents, at least, 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 publicly consulted 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 law investigation, non-public information is requested from ZOVAR by an authorised investigating officer, this information will be released by the director of the CIBG, after submission of a legal summons. The requirements imposed in the AVG are explicitly applicable to this.

If a subscriber requests non-public information from ZOVAR 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 referred to. If data is going to be issued, the party in question will be informed accordingly.

Confidential details will only be issued in order to provide proof to parties other than the subscriber, on the basis of the prior written permission of the subscriber.

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

9.5 Intellectual Property rights

This CPS is owned by ZOVAR. Unchanged copies of this CPS may be distributed and published without permission provided the sources are mentioned.

The certificates issued by ZOVAR will continue to be owned by ZOVAR. All intellectual property rights related to the certificates, including the rights relating to software, databases and logos are vested in ZOVAR. The rights cannot be transferred to third parties.

ZOVAR guarantees towards its subscribers that the certificates it has issued, including the corresponding and delivered documentation, do not violate intellectual property rights, including copyrights, brand rights and including copyrights, brand rights and any (potential) other intellectual property rights pertaining to the software used by ZOVAR, which are vested in its suppliers.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

With the introduction of the Online Administrative Business Act [Wet elektronisch bestuurlijk verkeer] the legislator has stipulated that with regard to liability a link has to be sought with the liability provisions in electronic legal transactions, in particular the liability of the certificate service provider that issues qualified certificates as laid down in Book 6 of the Dutch Civil Code.

In its capacity of certificate service provider the CIBG is liable for damage suffered by natural persons or legal entities, that reasonably trust an issued ZOVAR certificate and act on the grounds thereof, in conjunction with the accuracy, at the time of issue, of all details included in the certificate and the inclusion of all details prescribed for this certificate.

The CIBG can be held liable if it fails to register revocation of a ZOVAR certificate, including the updating and publishing of the CRL, and a person has acted accordingly in reasonable trust.

The CIBG cannot be held liable, on the basis of the above grounds, if it can submit proof that ZOVAR has not acted carelessly.

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

ZOVAR guarantees that procedures have been set up and measures implemented so that this CPS is complied with:

ZOVAR is liable in the event of intentional or negligent damage to a natural or legal person due to a failure to comply with the obligations under EU Regulation No. 910/2014 (eIDAS). ZOVAR is not liable for damage caused by the use of services that exceed the indicated limitations.

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 ZOVAR in relation to the purchase of certification services as laid down in the CPS. They must also observe instructions communicated to them by ZOVAR when the certificates are issued and/or made known to them at a later point in time.

If subscribers of certificate holders do not comply with the stipulations, this may result in damage for the ZOVAR, 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 4.5.1 of this CPS.

- The subscriber will only and exclusively purchase certification services from ZOVAR for its systems, databases.
- The subscriber guarantees that it is legally authorised to bind the organisation to ZOVAR. In addition, the subscriber can designate one or

more representatives, referred to as the applicant/certificate manager(s), for whom the subscriber will have final responsibility. This applicant/certificate manager(s) will be charged, on behalf of the subscriber, with the actual execution of the applications for and revocation of ZOVAR certificates in accordance with the procedures of the CPS. If the subscriber registration of (the organisation of) the subscriber is to be deleted, only the subscriber will be authorised to do so.

- The subscriber is always responsible for the choice and (physical) protection of its software, equipment and telecommunications facilities and the availability of its information and communication systems, with which it can set up the electronic communication within the organisation. For example, the subscriber will take suitable measures to protect its system against viruses and other software with inappropriate elements.
- The subscriber will issue correct, full and up-to-date details to ZOVAR, including details of the systems 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 other relevant changes, to ZOVAR no later than 24 hours after the change in question has occurred.
- The subscriber is obliged to set up and execute a procedure on the basis of which the subscriber or the applicant/certificate manager(s) can check whether the system of database for which a server certificate is being applied for is actually used for the organisation.
- The subscriber and certificate holder cannot transfer rights and obligations resulting from the relationship with ZOVAR to third parties, unless determined otherwise by ZOVAR.
- 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.[7]

The above obligations for the subscriber will, insofar as they can be designated as too uncertain, be developed in more detail in ZOVAR guidelines and/or more detailed regulations.

9.6.4 Relying party representations and warranties
No stipulation.

9.6.5 Representations and warranties of other participants
For representations and warranties of 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 ZOVAR, ZOVAR 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 by no later than within 24 hours. With this in mind a fallback scenario has been designed which is regularly tested. ZOVAR is not responsible for the non-availability of the services due to natural disasters or other circumstances for which ZOVAR cannot be held responsible.

7 In the event of calamities at ZOVAR, the Ministry of Health, Welfare and Sport will take adequate measures.

9.8 Limitations of liability

ZOVAR 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 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 do not concern the reasonable care taken by ZOVAR.
- Damage which arises due to subscribers, certificate holders and/or trusting parties not fulfilling the obligations described in this CPS.
- Damage as a consequence of misuse, loss, theft or other disappearance of the certificate, revocation code and the private key.
- Damage which arises due to the issue of a certificate on the grounds of incorrect information provided by the subscriber, insofar as ZOVAR 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, the software, the equipment or telecommunication facilities used by the subscriber.
- 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 performing the identification of the certificate manager 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 trusting party will be regarded as not having trusted the certificate reasonably, even if the trusting party has fulfilled all other obligations.

9.9 Indemnities

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

9.10 Term and Termination

9.10.1 Term

The CPS is valid as from the date of publication on the website www.zovar.nl. The CPS is valid as long as the services of ZOVAR continue, or until the CPS is replaced by a newer version. Newer versions will be designated by a higher version number (vX.x). In the event of drastic changes, the version number will be increased by 1. In the event of editorial changes, the version number will be increased by 0.1. Newer versions are to be published on the website of ZOVAR.

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 effect of the applicable CPS will be assessed and updated by ZOVAR 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 CIBG 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.

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, trusting parties and any other interested parties can submit a written change request supported by arguments. ZOVAR 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, changing legislation or suchlike. All change proposals are to be directly recorded. The party submitting the request will be sent a confirmation of receipt.

The management and staff will classify the change requests. Where necessary, specialist legal or technical knowledge will also be applied. In the event of 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
ZOVAR publishes the CPS on the website: www.zovar.nl. In addition, the CPS can be requested using the contact information referred to in section 1.5.1 'Contact details'. This application can only be made in writing.

9.13 Dispute Resolution Provisions

The CPS will indicate the interpretation of the ZOVAR stipulations. This interpretation must take account of the general objective of ZOVAR. If this clarification does not produce a satisfactory result for the party/parties involved, the conflict will be submitted to a conflict mediator who is acceptable to all parties involved 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 exclusively to the competent court in The Hague.

In the event of complaints concerning services delivered by ZOVAR, the complaint can be submitted in writing to the CIBG via the complaint form on www.cibg.nl or by post, for the attention of the cluster head responsible for ZOVAR, stating the reference 'Complaint'. ZOVAR 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 you are not satisfied with the handling of the complaint, you can contact the National Ombudsman at Postbus 93122, 2509 AC Den Haag, or via the website www.nationaleombudsman.nl

If a conflict arises between two purchasers of services offered by ZOVAR, the cluster head of ZOVAR 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 ZOVAR and this CPS are subject to Dutch law.

9.15 Compliance with Applicable Law

As the implementing body of the services of ZOVAR the CIBG 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 which is related to its capacity of TSP and the services that it delivers. All this with due observance of the fact that the ZOVAR as part of the Ministry of Heath, Welfare and Sport 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 on the basis of the following points of departure:

- 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, if applicable, the source of the information with an empty line in between.

Abbreviation	Term	Definition
	Subscriber	Healthcare insurer of healthcare administration office in accordance with the definition used by ZOVAR, which purchases certificate services from ZOVAR. The subscriber is the party on whose behalf a server/service 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.
	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. See also 'Private key' and 'Public key'.
	Authentication	The 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'.
	Authentication certificate	A certificate that should exclusively be used for authentication - or electronic identification.
	Authorisation	Granting someone the authority to carry out certain activities (examples of activities: inspecting, modifying or processing details).
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.

Abbreviation	Term	Definition
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
	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 concerning the confidentiality and authenticity and/or electronic signature and therefore confirms the person's identity. A certificate is encrypted with the private key of the Certification Authority which has issued the public key, whereby the certificate cannot be falsified. A certificate contains at least: the identification and the country of establishment of the issuing certificate service provider; the name of the signatory; the statement of the times at which the period of validity of the certificate starts and ends; the identity code of the certificate; any restrictions concerning the use of the certificate, and any limits relating to the value of transactions for which the certificate can be used.
	Certificate holder	A natural person or legal entity on whose behalf a certificate has been issued and whose identity can be established using the certificate. In the case of server certificates the certificate holder will be a machine or server.
	Certificate manager	The role of certificate management is only important for products whereby the certificate holder is a system or a group/position, in other words for server certificates. In the case of these products, ZOVAR has opted for the applicant of these products to act as certificate manager as well, on behalf of a subscriber.

Abbreviation	Term	Definition
	Certificate profile	A description of the content of a certificate. Each type of certificate (signature, confidentiality, etc.) has its own content and, with that, its own description. This contains, for example, agreements regarding names, etc.
CP	Certificate Policy *certifica-tion-policy*	A document with a collection of requirements referred to that indicates the frameworks within which ZOVAR issues certificates. The CP is drawn up by the Policy Authority of the PKI for the Government. By using, among other things, the CP, certificate holders and trusting parties can determine how much trust they place in ZOVAR.
CRL	Certificate Revocation List *certificate revocation list*	A list of withdrawn (= revoked) certificates. This list can be accessed and consulted by the general public. The list is made available by and under the responsibility of ZOVAR. The CRL is itself also electronically signed by the CA of ZOVAR.
	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 ZOVAR 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 CIBG regarding all aspects of the services. The CPS describes how ZOVAR 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 presumably lost private key or bearer; • Stolen or presumably stolen private key or bearer; • Destroyed private key or bearer. A compromise constitutes a reason for placing a certificate on the Certificate Revocation List.
	Directory service	The directory service is a service of ZOVAR which is intended to make issued certificates available and accessible on the Internet.
	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.

Abbreviation	Term	Definition
	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 Standards Institute	The ETSI is an independent institute in the field of telecommunications standardisation.
	Birth name	The birth name is the name as included in the passport or identity document (also known as maiden name or family name).
	Authorised applicant	A person who is authorised by the legal representative of the subscriber to submit applications for the issue of certificates on behalf of the subscriber.
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 business 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.
	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 certificates.
	Private key	See 'Private key'.
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 ZOVAR. See also 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.

Abbreviation	Term	Definition
	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 ZOVAR that carries out the registration work in order to process the certificate applications.
	Revocation	Revocation concerns making a certificate invalid (revocation). 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).
	Key(s)	See respectively: • Asymmetric key pair • Private key • Public key
	Key pair	See also asymmetric key pair.
	Server certificate	A certificate with which a service or device, for example a server is linked to a legal entity or other organisation. In the case of a server the certificate is submitted to a browser which seeks access to the server. In this way, a trusting party can be certain regarding the identity of the server's owner. A server certificate is not a qualified certificate.
	Root 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 root certificate.
RDI	Rijksinspectie Digitale Infrastructuur	Dutch Authority for Digital Infrastructure Supervisor of laws and regulations in the field of: available technical infrastructures, security and resilience of networks and services, secure and reliable devices
TSP	Trusted Service Provider *certificatiedienst ☐ verlener*	A natural person or legal entity that issues the certificates and/or provides other services connected to the electronic signatures, including identity and confidentiality within the meaning of Article 1.1 under tt of the Telecommunications Act.
UZOVI	Insurance Company Identification	The address details and the unique UZOVI number are registered and maintained in the UZOVI register. Since 1 January 2006 the register has contained the details of the care insurers, authorised insurance intermediaries, healthcare administration offices, label organisations and branches.
	Confidentiality	The guarantee that details are actually and 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.

Abbreviation	Term	Definition
	Trusting party	The natural person or legal entity that is the recipient of a certificate and that acts in trust on the basis of that certificate.
	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 ZOVAR.
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 citizen 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 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.
X.509	X.509	This is an electronic certificate that is compiled in accordance with a standardised structure.
	Healthcare administration office	A Wlz implementing body designated for certain region pursuant to the second section of Article 4.2.4;
	Health insurer	This means: **1°.** Wlz implementing body as referred to in Article 1.1.1 of the Long-Term Care Act [Wet langdurige zorg] (Wlz); **2°.** healthcare insurer as referred to in Article 1, under b, of the Healthcare Insurance Act; **3°.** insurance company as referred to in the Solvency II Directive insofar as this company offers or implements insurance policies pursuant to which the insured risk is the need for care to which, by virtue of or pursuant to the Long-Term Care Act, no entitlement exists and whereby the insured performance exceeds that arranged by virtue of or pursuant to the Healthcare Insurance Act; Solvency II Directive 2009/138/EC is the new, risk-based supervision framework for insurers that came into effect on 1 January 2016. The primary purpose of the framework is to protect the interests of policyholders. This is achieved via quantitative capital requirements, qualitative requirements on the quality of operations and transparency to the public and the regulator. Solvency II does not apply to funeral expenses and benefits in kind insurers and most small insurers.