CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

PKI DISCLOSURE STATEMENT (PDS)

UZI-register

Version 1.2

Date: 05-11-2018
Status: Final

Contents

Version history

This PKI Disclosure statement has the following revisions:

Version	Date	Status	Description
1.0	08-05-2017	Final	First published version
1.1	02-10-2018	Final	General Data Protection Regulation (De Algemene verordening gegevensbescherming)
1.2	05-11-2018	Final	Groepscertificaten (Group certificates) available

Accord TSP Management
Versie: 1.2
Datum: 05-11-2018

1. Introduction

This document is the PKI Disclosure Statement of the UZI-register, hereafter referred to as PDS. The document is intended for subscribers, certificate holders and relying parties of the UZI-register. This document does not replace or modify the Certification Practice Statement (CPS). The subscriber and the cardholders should explicitly agree with the CPS-UZI register during the application process.

The purpose of this document is to summarize the main points of the CPS UZI-register for subscribers, certificate holders and relying parties of the UZI-register.

2. CA Contact information.

Information about this PDS or the service of the UZI-register can be obtained from the contact details below. Comments on the present PDS can be addressed to the same address.

Contact information UZI register:

Rijnstraat 50
2515 XP The Hague
Tel: 0900 - 232 4342

PO Box 16114
2500 BC The Hague

info@uzi-register.nl

www.uziregister.nl

3. Type of Certificates, Validation procedure and certificate useage.

The UZI-register issues 3 types of certificates under the Root of PKI Overheid:

1. Persoonlijke certificaten (Personal certificates);
2. Beroepsgebonden certificaten (Profession bound certificates);
3. Groepscertificaten (Group certificates).
4. Server certificaten (Server certificates).

The full description of the type of certificates supported by the UZI register and the validation procedures are described in the CPS-UZI register, which can be found at www.zorgcsp.nl

4. Limitation of the use of the reliability of certificates (Reliance limits)

Not applicable.

5. Obligations for subscribers

Below are the main obligations of the subscriber. The full list is listed in the CPS UZI-register, which can be found on https://www.zorgcsp.nl

- The subscriber guarantees that all information provided is accurate and complete. This concerns data related to subscriber registration, certificate application and other data. Changes to the data, such as a name change at the Chamber of Commerce, will be reported to the UZI register by the subscriber within 24 hours.
- If any of the following occurs up to the end of the validity period indicated in the Certificate the subscriber must immediately revoke the certificate:
    - the Subject's Private Key has been potentially or actually lost, stolen or compromised.
    - control over the Subject's Private Key has been lost due to potential or actual compromise of activation data (eg PIN code) or other reasons.
    - inaccuracy or changes to the Certificate content, as notified to the Subscriber.

This can be achieved on: https://www.zorgcsp.nl

- Ensure that if the Subscriber or Subject generates the Subject's Key Pair, only the Subject holds the Private Key.
- Generate the Key Pair in a safe environment.

6. Obligations of the relying parties for the verification of the certificate status

Relying parties are required to check the current status (revoked / unrevoked) of a certificate by consulting the most recently published Certificate Revocation List (CRL) or through the On-line Certificate Status Protocol (OCSP) facility.

Relying parties are also required to check the electronic signature with which the CRL is signed, including the associated certification path.

The status of a certificate issued by the UZI register has been published in the CRL; or available through the OCSP facility, which can be found at www.zorgcsp.nl

7. Limited warranty and disclaimer/Limitation of liability

The UZI register is in the role of trust service provider liable for damage that natural persons or legal persons, who reasonably trust and act on a certificate issued by the UZI register, experience in context with:

- The accuracy, at the time of issue, of all data included in the certificate and the inclusion of all data required for this certificate.
- The fact that, at the time of issue, the person indicated in the certificate as the signatory was the holder of the data for creating electronic signatures.

In addition, the UZI register can be held liable if it fails to register revocation of the certificate, including updating and publishing the CRL, and has acted in a reasonable faith by a person. The UZI register can't be held liable on the basis of foregoing grounds if they can provide evidence that the UZI register has not acted negligently.

8. Applicable agreements, certification practice statement, Certificate

The UZI-register is a Trust Service Provider (TSP) which issues certificates under the programme of requirement for the PKI for the government.

The document below is available at https://www.zorgcsp.nl

1. Certification Practice Statement (CPS)

9. Privacy policy

The information obtained from the UZI register about a person, being a natural person or legal person, is treated confidentially. The requirements of the General Data Protection Regulation (GDPR) are explicit applicable.

The published certificate information is only publicly available through the search function on the website. The information related to published and revoked certificates is limited to what is stated in Chapter 7 "Certificate, CRL and OCSP profiles" of the CPS-UZI registry.

10. Reimbursement directives

Not applicable

11. Governing Law and settlement of disputes clauses

The UZI register is a Trust Service Provider (TSP). Because of this the UZI register is bound by all European and national laws and regulations relating to her capacity as TSP and the services it provides.

12. CA and certificate directory licenses, confidentiality trademarks and audit

The UZI-register is subject to a yearly compliance audit by a accredited auditor against the requirements of :

- European regulation Nr. 910/2014 (eIDAS)
- The program of requirements PKI Overheid
- ETSI EN 319 411-1 and ETSI EN 319 411-2

Proof of successful certification can be found by viewing the BSI certificates of compliance on our website: www.uzi-register.nl

13. Abbreviations and Terms

Abbreviation /Term	Description
CA	Certification Authority
Certificate	An electronic document that uses a digital signature to bind a public key and an identity.
CP	Certificate Policy
CPS	Certification Practice Statement

CRL	Certificate Revocation List
PKI	Public Key Infrastructure. A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA).
Subscribers	A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber or Terms of Use Agreement
Relying Party	Any natural person or Legal Entity that relies on a Certificate by verifying the authenticity of a subscriber based on a certificate of PKIoverheid. A relying party can also be a subscriber.