Certification Practice Statement

Version 1.24 16-01-2025

This is the official version of the Cleverbase Certification Practice Statement.

Hierarchy of documentation

In case of disputes between documentation, the following hierarchy exists:

- The certification practice statement
- PKI disclosure statement
- The terms & conditions in Dutch
- The terms & conditions in English
- The product conditions in Dutch
- The product conditions in English
- Other public outings by Cleverbase

Table of Contents

1 Introduction

1.1 Overview

PKIoverheid is a public key infrastructure (PKI) set up at the initiative of the Dutch government, for the purpose of enabling and supporting electronic signatures, electronic authentication, and confidential electronic communication. Certificates issued within this PKI are highly reliable. Several trust service providers (TSPs) operate within this PKI, and are trusted to issue certificates. Root certificates in this PKI are signed by the Staat der Nederlanden (State of the Netherlands).

This CPS is applicable to all certificates issued within this CA hierarchy:

- Staat der Nederlanden Root CA - G3
  - Staat der Nederlanden Burger CA - G3
    - **Cleverbase ID PKIoverheid Burger CA - G3**
      - Authentication (2.16.528.1.1003.1.2.3.1)
      - Non-repudiation (2.16.528.1.1003.1.2.3.2)
      - Encryption (2.16.528.1.1003.1.2.3.3)

Cleverbase acts as a TSP within PKIoverheid. Cleverbase aims to provide citizens as well as businesses with the certificates they require to reliably and confidentially exchange information with each other, or with the government. Primarily, certificate applicants register remotely by means of a mobile application that is developed and provided by Cleverbase. Using this app, a video call is made to verify the applicant's identity and identifying documents, after which Cleverbase issues the certificates they have applied for.

Vidua is a registered trade name owned by Cleverbase ID B.V. Cleverbase uses Vidua as the public brand name for its products and in its product outings. All TSP operations are performed by Cleverbase in accordance with the provisions of this document. In order to provide the end users with a consistent experience, the service desk and registration office operated by Cleverbase also use the Vidua brand name.

All certificate related key material is stored in a Trustworthy System Supporting Server Signing (TW4S). Cleverbase supports two TW4S-sytems. For both systems holds:

- The private key can only be used within a Hardware Security Module (HSM) in which it resides and assures SCAL2;
- These HSMs are located in data centres, and are configured to grant exclusive control of keys to the respective certificate holder;
- The sole control can be exerted by means of a mobile application which is tied to the certificate holder’s smartphone, and secured by a PIN of their choosing;
- The HSMs are operated by Cleverbase;
- The HSMs are physically and logically under Cleverbase's sole control.

The main TW4S system makes use of I4P's Trident HSMs and a SIC app managed by Cleverbase. The second TW4S system makes use of Thales HSMs and a SIC app managed by Ubiqu Access B.V. This second system is still maintained for users who use this old SIC app and for some internal use cases.

1.2 Document Name and Identification

This document is Cleverbase's Certification Practice Statement (CPS). It is based on the PKIoverheid Programme of Requirements (PoR) (available at PKIoverheid Programma van Eisen), ETSI standards EN 319 411-1 and EN 319 411-2 (both available at https://www.etsi.org/standards), Regulation (EU) 910/2014 (eIDAS) (32014R0910 - EN - EUR-Lex), and Regulation (EU) 2024/1183 (eIDAS 2.0) (32024R01183 - EN - EUR-Lex). Its structure is modelled after RFC 3647.

This CPS sets out the practices Cleverbase employs with regards to the issuance of certificates in the Citizen Domain. It falls under the scope of the Certificate Policy (CP) of the PKIoverheid Programme of Requirements for domain G3 Legacy Citizen certificates (previously 3c). Supported certificate uses are authenticity, non-repudiation and encryption. The PKIoverheid PoR assigns a separate Object Identifier (OID) to each combination of the target domain and intended certificate use . The Citizen Domain CP covers the following OIDs:

Use	Authenticity	Non Repudiation	Encryption*
OID	2.16.528.1.1003.1.2.3.1	2.16.528.1.1003.1.2.3.2	2.16.528.1.1003.1.2.3.3

* Cleverbase does not currently issue encryption certificates to clients.

1.3 PKI Participants

The following participants in PKIoverheid are relevant here:

1.3.1 Certification Authorities

Cleverbase is the Certification Authority (CA) responsible for issuing the certificates specified in section 1.2.

1.3.2 Registration Authorities

Cleverbase is the Registration Authority (RA) responsible for evaluating applications for certificates, which includes establishing the identity of the certificate applicant. Once specialised Registration Authority staff members, known as registration officers, have approved the application, the CA issues the requested certificate. The applicant becomes a subscriber upon receiving the certificate.

1.3.3 Subscribers

Subscribers are users of our services and enter into an agreement with Cleverbase. A subscriber is a natural person.

The subscriber is also the certificate holder. The certificate holder is the entity stated in the subject field of the certificate. The subscriber in the Citizen Domain will have accepted the General Terms and Conditions, as well as had their identity established and their certificate application approved by the RA.

1.3.4 Relying Parties

A relying party may be any natural or legal person who, as a recipient of a certificate issued by Cleverbase, acts in reliance on that certificate and/or any digital signatures verified using that certificate. This CPS contains requirements for relying parties, please refer to section 4.5.2 and 4.9.6.

1.3.5 Other Participants

Other participants under this CPS include regulatory and supervisory authorities, suppliers of hardware, software and equipment, as well as other supporting organisations. In particular, these include:

- The Policy Authority (PA). The PA's task is to develop and maintain the framework of standards that underlies PKIoverheid, and to supervise, regulate and monitor its implementation. Logius fulfils this task on behalf of the State of the Netherlands.
- Ubiqu Access B.V. (Ubiqu). Cleverbase has entered into a cooperation agreement with Ubiqu. Within this agreement, Ubiqu provides tokens that are to be issued to personal certificate holders. These tokens consist of a set of private keys stored in the trustworthy system supporting server signing (TW4S), and the Authentication App on the certificate holder's mobile phone. Using this app, certificate holders can exert exclusive control over their private keys. Although Ubiqu administers this system, Cleverbase bears full responsibility for its use and operation.
- Cleverbase's own TW4S-system also stores a set of private keys in a trustworthy system support server signing (TW4S). Usage of these keys can be initiated with the Vidua app on the certificate holder's mobile phone. Using this app, certificate holders exert full control over their private keys. The private keys are stored in EN 419 221-5 certified devices and usage of private keys is enforced by EN 419 241-2 certified SAM. Cleverbase bears full responsibility for its use and operation.

Cleverbase ensures that all participants meant under this paragraph act in accordance with the terms and policies laid down in this CPS. Cleverbase has appropriate controls in place to maintain adherence to said terms.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificate usage differs per certificate type. Before elaborating on each certificate type, the following general remarks must be made:

- Certificates must be used in accordance with the general terms and conditions that apply.
- No restrictions apply as to the value of the transaction for which the certificate is used.
- Certificates may be used in interactions with the State of the Netherlands as well as with other natural or legal persons.

Certificates in the Citizen Domain type may be used by individual natural persons.

Different certificates are issued per type for authentication, confidential communication and electronic signatures. Certificates may only be used for the purpose for which they were issued. The table below shows these purposes per certificate. These purposes of use correspond to the keyUsage field in the certificate.

	authenticity	**encryption**	**signature**
Citizen (G3) Domain (section 3c PoR)	digitalSignature	keyEncipherment dataEncipherment	nonRepudiation

1.4.2 Prohibited Certificate Uses

All other certificate usage types than the ones stated in section 1.4.1 are prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Cleverbase assesses this CPS and corrects any errors or omissions at least once a year. Intended major revisions of this CPS will be established by the TSP´s management.

Minor/administrative revisions will be done without prior announcement. Revisions that might affect the acceptance of the service or its terms will be communicated to subscribers and relying parties on the public website prior to them coming into force.

With minor revisions the version number will increase by 0.1, major revisions lead to a new version.

1.5.2 Contact Person

Please address any enquiries about the CPS or other communications to info@cleverbase.com

Or, alternatively, to:

Cleverbase ID B.V.
Maanweg 174
2516AB, 's-Gravenhage

1.5.3 Person Determining CPS Suitability for the Policy

Please refer to section 1.5.1.

1.5.4 CPS Approval Procedures

Please refer to section 1.5.1.

1.6 Definitions and Acronyms

Abbreviation	Definition
CA	Certificate Authority. The system entity that issues and manages digital certificates to authenticate the identity of users
RA	Registration Authority. The system entity responsible for verifying the identity of individuals before the issuance of digital certificates by a Certificate Authority
CRL	Certificate Revocation list. A list of certificates that have been revoked by the issuing Certificate Authority.
OCSP	Online Certificate Status Protocol. A protocol which checks the status of a requested certificate.
CPS	Certification practice statement.This document, outlining the policies, procedures, and practices employed by Cleverbae in issuing and managing digital certificates within the framework of trust services.
PKI	Public Key Infrastructure. A digital framework for issuing and managing certificates.
TSP	Trust Service Provider. The entity that offers electronic trust services while adhering to regulatory standards and requirements.
HSM	Hardware Security Module. Dedicated hardware device that securely generates, stores, and manages cryptographic keys used for digital signatures and other cryptographic operations to enhance the security of electronic transactions
TW4S	Trustworthy Systems Supporting Server Signing.
OID	Object Identifier. A unique number representing a certain object and/or name.

2 Publication and Repository Responsibilities

2.1 Repositories

Cleverbase has an electronic repository holding:

- Documentation dissemination;
- Certificates;
- Certificate status service.

The CA public key is not part of Cleverbase's electronic repository but can be retrieved via https://cert.pkioverheid.nl/.

2.2 Publication of Certification Information

The following information is accessible via the documentation dissemination service via vidua.nl/legal:

- this Certification Practice Statement;
- the general terms and conditions;
- the product conditions;
- the PKI Disclosure Statement;
- test certificates;
- the privacy statement.

2.3 Time or Frequency of Publication

The electronic repository is available 24 hours a day and 7 days a week. The maximum recovery time for the Documentation Dissemination Service is 24 hours. The maximum recovery time for the Certificates and Certificate status service is four hours.

- The Certification Practice Statement is published after a revision.
- The general terms and conditions are published after a revision.
- The PKI Disclosure Statement is published after a revision.
- The certificates are published immediately after a successful registration.
- The certificate status service is updated within four hours after a successful revocation.

2.3.1 Accessibility of repositories

- Earlier versions of the CPS, the general terms and conditions and product conditions are available on the Cleverbase public website vidua.nl/legal.
- The (end user) certificates are accessible for certificate holders and can only be shared with relying parties with consent by the certificate holder.

2.4 Access Controls on Repositories

The electronic repository is accessible as described in the previous section. It is secured against unauthorised modifications. Only the TSP has writing permissions for the electronic repository.

3 Identification and Authentication

This section describes the identification and authentication processes during initial registration and prolongation.

3.1 Naming

3.1.1 Types of Names

The certificate holder is identified in the subject field of the certificate with a distinguished name (DN) as meant in X.509. Required DN components differ for various certificate types:

	Citizen (G3) Domain
serialNumber	personal number, uniquely identifying the certificate holder in Cleverbase's systems
commonName	certificate holder's name, formatted as follows: [all given names in full] [maiden name / last name]
countryName	certificate holder's country of residence according to the nationality of the identity document submitted
givenName	all given names of the certificate holder
surname	the certificate holder's surname (maiden name / last name)

Please refer to the certificate profiles as described in Chapter 7 of this document for more information.

3.1.2 Need for Names to be Meaningful

Each DN has a meaningful relation to the represented entity.

3.1.3 Anonymity or Pseudonymity of Subscribers

Pseudonymous or anonymous certificates are not allowed.

3.1.4 Rules for Interpreting Various Name Forms

All names contained in the commonName, givenName, and surname are copied directly from the identification document, with the following exceptions:

- In case the commonName exceeds the character limit, one or more first names will be replaced with initials, starting with the last full first name, until the commonName no longer exceeds the character limit. If first names are replaced by initials in the commonName, the same is done for the givenName.
- In case the identification document contains a non-Latin alphabet and a Latin transliteration, the Latin transliteration will be used as default.
- Capital and non-capital characters are considered as identical characters.
- In case the names contain special characters that are not part of the supported character set, MES-1, Cleverbase will transliterate the character to a supported character. Transliteration will be done according to a transliteration list. If the character is not present on the transliteration list, these characters will be transliterated to the closest available character in the 26-character Latin alphabet.

The countryName is saved in the two-letter ISO 3166-1 country code notation.

3.1.5 Uniqueness of Names

Each DN is unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

Cleverbase registers natural persons remotely, using a dedicated mobile app. Cleverbase requires the use of a passport or national identity card. Driver's licenses or other identification documents (visa, residents permits etc.) are explicitly excluded. The list of countries that are currently supported is maintained on the Vidua website.

NOTE: For the listed countries, identity document models are supported if they comply with the International Civil Aviation Organization (ICAO 9303) standard on use of NFC and Visual Inspection Zone. Cleverbase can make exceptions for other identity document models based on comparable security features. Cleverbase will always conduct an intake before supporting a specific ID-document model.

The primary registration proces is a hybrid attended remote identity proofing process in accordance with ETSI TS 119 461, as it uses NFC scanning. A secondary process option using MRZ scanning is a manual attended remote identity proofing process in accordance with ETSI TS 119 461.

The initial remote identity validation is performed using a mobile phone app that allows the TSP to establish the identity remotely and then to install the token on the mobile phone. As a minimum, the registration process comprises the following actions:

1. The SIC is installed on the phone in the form of:
    - the Vidua app with its own TW4S or;
    - the Authenticate app, which is part of the Ubiqu token.
2. The user accepts the Terms & Conditions for users
3. The prospective certificate holder chooses a PIN, and a link is established between PIN, phone, and the (future) identity.
4. The email address of the prospective certificate holder is registered.
5. The user accepts the product conditions for registration.
6. A selfie of the prospective certificate holder is made and sent to the Cleverbase server.
7. A photo of the prospective certificate holder's valid identity document is made and sent to the server, together with the personal data required for registration.
8. The prospective certificate holder uses the Vidua application (iOS or Android) to read the NFC chip in the identity document after which the data is sent to the Cleverbase server. Cleverbase applies Near Field Communication (NFC) in accordance with the International Civil Aviation Organization (ICAO) Doc 9303 standard. Dutch registrants who fail to scan the RFID-chip can skip this check, but are subject to extra validations in the videocall.
9. The app sets up a video connection with a registration officer. The registration officer performs the following checks before and during the video call:
    - The registration officer checks the quality of the video connection and may give instructions regarding ambient light and sound;
    - The registration officer checks the data submitted against the picture of the identity document;
    - The registration officer verifies authenticity and validity of the identity document, checking, among other things, whether it has been recorded stolen or missing with an authentic source if publicly available;
    - The registration officer verifies the authenticity of the identity document using optical, audible and/or automated authenticity features;
    - The registration officer verifies the prospective certificate holder's identity;
    - The registration officer checks whether the applicant has applied for a certificate with Cleverbase before. (In this case, existing certificates are revoked when issuing the new certificates);
    - The registration officer requests the applicant to read out a unique code and to express the unambiguous will to apply for a certificate.
10. If all checks have positive results, the registration officer approves the certificate application.

11. The prospective certificate holder reconfirms their PIN, thereby proving possession of the private key. The prospective certificate holder must confirm their registration within 48 hours after the video call to ensure freshness of information. After 48 hours of inactivity, the registration attempt will automatically expire.
12. A second registration officer reviews the certificate application and approves the issuance of a certificate if all requirements are met.
13. The certificate holder receives an activation link and a revocation code by email:
    - The activation link is used to activate the profile to complete the registration and enable use of keys and certificates;
    - The revocation code is to be used if the user decides to revoke the certificate later on.

The TSP has controls in place for the continuous improvement of the process described above, including, as a minimum:

- Both Cleverbase's internal auditor and external auditors take periodic checks of old files. All files processed by registration officers that appear to have inadvertently approved one or more certificate applications are reconsidered.

3.2.1 Method to Prove Possession of Private Key

Please refer to section 3.2.

3.2.2 Authentication of Organization Identity

Not supported for certificates in the Citizen Domain.

3.2.3 Authentication of Individual Identity

Please refer to section 3.2.

3.2.4 Non-verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

Not supported for certificates in the Citizen Domain.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

Re-key of certificates is not supported.

3.3.1 Identification and Authentication for Routine Re-key

No stipulation.

3.3.2 Identification and Authentication for Re-key After Revocation

No stipulation.

3.4 Identification and Authentication for Revocation Requests

Certificate holders can identify for revocation requests in any of the following ways:

- Certificate holders use the revocation code provided to them through email and enter it in the public section of Cleverbase's website. The revocation is used as a means for identification and authentication.
- Certificate holders contact Cleverbase by phone and answer some questions relating to their personal data, by which the revocation officer establishes their identity.
- Certificate holders send an email to Cleverbase, providing their full name, date of birth, place of birth.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

A natural person with a valid identity document can apply for a certificate in the Citizen Domain. Cleverbase maintains an list of supported identity documents [section 3.2] on a risk based approach. As such Cleverbase retains the right to disallow the use of a specific identity document at its sole discretion

4.1.2 Enrolment Process and Responsibilities

Prospective certificate holders apply for certificates in the Citizen Domain. At the moment of application, they enter into an agreement with Cleverbase. Applicants can only complete the application after having agreed with the general terms and conditions published in accordance with section 2.2. The initial identity validation and certificate issuance will always be subject to the CPS version and product conditions that are accepted at the beginning of the registration process. Should a new CPS or new product conditions be published between acceptance of previous versions and completion of the process, the accepted versions shall prevail.

During the application process prospective certificate holders' identities are verified as described in section 3.

Certificate holders can retrieve certificates at the TSP's web portal after login.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Please refer to section 4.1.

4.2.2 Approval or Rejection of Certificate Applications

Please refer to section 4.1.

4.2.3 Time to Process Certificate Applications

The usual time to process the application is within a day. This can take up to 5 working days when additional personal identity validation is required.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The CA validates the completion of the process described in section 3.2 before issuance of a certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Subscriber receives an email notification after issuance of the certificates.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Certificates in the Citizen Domain are accepted by implication.

4.4.2 Publication of the Certificate by the CA

The certificates are published in the electronic repository, please refer to section 2.2.

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

Any agreement entered into by a subscriber and a certificate holder entails their obligation to use the certificate in accordance with this CPS, the general terms and conditions, and the usage purposes described in the certificate (please refer to section 1.4).

4.5.2 Relying Party Public Key and Certificate Usage

Before trusting a certificate, relying parties should check the:

1. certificate's validity and the entire certificate chain belonging to it up to the root certificate at the moment they trust it, by consulting certificate status information (please refer to section 4.1);
    - For a certificate to be relied upon as an EU qualified certificate, the CA/trust anchor for the validation of the certificate shall be as identified in a service digital identifier of an EU trusted list entry with the service type identifier https://uri.etsi.org/TrstSvc/Svctype/CA/QC/. ETSI TS 119 615 provides guidance for relying parties on how to validate a certificate against the EU trusted lists.
2. certificate usage in accordance with the usage purposes described in the certificate (please refer to section 1.4) and general terms and conditions and product conditions.

4.6 Certificate Renewal

Certificate renewal is not supported. If a certificate holder applies for a new certificate with a new key pair, the same procedures as during initial certificate application are followed. Any changes in terms or conditions resulting from interim reviews are pointed out during application.

4.6.1 Circumstance for Certificate Renewal

No stipulation, please refer to section 4.6.

4.6.2 Who May Request Renewal

No stipulation, please refer to section 4.6.

4.6.3 Processing Certificate Renewal Requests

No stipulation, please refer to section 4.6.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation, please refer to section 4.6.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation, please refer to section 4.6.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation, please refer to section 4.6.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation, please refer to section 4.6.

4.7 Certificate Re-key

Certificate re-key is not supported.

4.7.1 Circumstance for Certificate Re-key

No stipulation, please refer to section 4.7.

4.7.2 Who May Request Certification of a New Public Key

No stipulation, please refer to section 4.7.

4.7.3 Processing Certificate Re-keying Requests

No stipulation, please refer to section 4.7.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation, please refer to section 4.7.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation, please refer to section 4.7.

4.7.6 Publication of the Re-keyed Certificate by the CA

No stipulation, please refer to section 4.7.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation, please refer to section 4.7.

4.8 Certificate Modification

Modification of certificate data is not included in the service. The general terms and conditions oblige certificate holders to have their certificates revoked if certificate data is no longer correct. They can apply for a new certificate with modified data if desired.

4.8.1 Circumstance for Certificate Modification

No stipulation, please refer to section 4.8.

4.8.2 Who May Request Certificate Modification

No stipulation, please refer to section 4.8.

4.8.3 Processing Certificate Modification Requests

No stipulation, please refer to section 4.8.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation, please refer to section 4.8.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation, please refer to section 4.8.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation, please refer to section 4.8.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation, please refer to section 4.8.

4.9 Certificate Revocation and Suspension

A certificate can be revoked under certain circumstances. The TSP will then add it to the CRL and an OCSP request will return its status as revoked. This section describes under which circumstances, by whom and in which way a certificate can be revoked.

4.9.1 Circumstances for Revocation

A certificate can be revoked under the following circumstances:

1. The subscriber requests a revocation;
2. Confidentiality of the private key corresponding to the certificate's public key was presumably compromised. Cases include those in which a mobile phone on which the Authenticate or Vidua app was installed was lost or stolen, or confidentiality of the PIN was compromised;
3. The certificate holder fails to comply with their obligations based on this CPS or the agreement closed with them;
4. Information in the certificate is not or no longer correct and up-to-date, or information in the certificate is misleading;
5. There are indications that the certificate is being misused;
6. The certificate appears not to have been issued following the proper procedures in retrospect;
7. The TSP terminates its activities with no other TSP taking over the CRL and OCSP services;
8. The TSP suspects the CA private key used to issue the certificate to be compromised;
9. The policy authority of PKIoverheid determines that the certificate does not meet requirements;
10. Revoking the certificate can help prevent or fight a calamity;
11. Other circumstances occur which, in the TSP's view, justify revoking the certificate in order to sustain trust in the public key infrastructure;
12. The subscriber, who is a natural person, has passed away;
13. The subscriber indicates that the original certificate request was not authorized and does not retroactively grant authorization;
14. The certificate was issued in violation of the then-current version of these requirements.

4.9.2 Who Can Request Revocation

A certificate may be revoked at the initiative of:

1. the TSP itself;
2. the certificate holder;
3. the subscriber.

As the TSP can itself initiate certificate revocation, anyone who is aware of a circumstance that could lead to revocation may inform the TSP without obligation. Revocation can then proceed if the TSP sees a reason for it.

4.9.3 Procedure for Revocation Request

Certificate holders can revoke their own certificates through the TSP's web portal at any moment using the revocation code provided to them by email during application. Each of the parties mentioned in section 4.9.2 can request revocation by contacting the TSP's customer service by phone during opening hours. For non-urgent revocation requests outside office hours, an email can be sent to the customer service. These emails will be processed during opening hours. For office hours and contact details, please refer to the website, https://vidua.nl.

If the TSP revokes a certificate on its own initiative, it will explain why it does so.

If the revocation service is disrupted for whatever reason, the TSP ensures the disruption is corrected within 24 hours.

If the TSP receives information that in itself does not imply a revocation request but contains indications of a problem concerning a certificate, the TSP will set up an investigation that can possibly entail revocation within 24 hours, or as fast as possible during office hours.

Certificate holders who themselves revoke certificates by using the web portal, by phone or by email receive confirmation as soon as revocation is successful.

When a certificate holder issues a revocation request, they must identify and authenticate themselves. The method for this differs per method for revocation and is described in section 3.4.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time Within Which CA Must Process the Revocation Request

Revocation is effectuated within a maximum of 24 hours after receipt of an authenticated request for revocation as specified in section 4.9.3.

If a revocation request cannot be confirmed within 24 hours, Cleverbase will determine a course of action in coordination with the supervisory body RDI.

4.9.6 Revocation Checking Requirement for Relying Parties

The CRL and OCSP are publicly available at the repository (please refer to section 2.1).

4.9.7 CRL Issuance Frequency (if applicable)

The CRL is updated at least every 24 hours. Please refer to section 2.3.

4.9.8 Maximum Latency for CRLs (if applicable)

No stipulation.

4.9.9 On-line Revocation/Status Checking Availability

Please refer to section 2.1.

4.9.10 On-line Revocation Checking Requirements

Please refer to section 2.1.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

Revocation of the 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;
- Incidents reported to Logius by third parties which may indicate key compromise.

All indicators are registered, analysed, and followed up accordingly. In case of a key compromise, the certificate holder must revoke their certificate immediately through one of the methods described in section 3.4 Identification and Authentication for Revocation Requests.

4.9.13 Circumstances for Suspension

The TSP does not support certificate suspension. Certificates cannot be revoked or deactivated temporarily or reinstated after revocation.

4.9.14 Who Can Request Suspension

No stipulation, the TSP does not support certificate suspension.

4.9.15 Procedure for Suspension Request

No stipulation, the TSP does not support certificate suspension.

4.9.16 Limits on Suspension Period

No stipulation, the TSP does not support certificate suspension.

4.10 Certificate Status Service

4.10.1 Operational Characteristics

The TSP offers a certificate status service allowing to check the validity of certificates. The addresses for consulting this service are shown in the certificate and follow here:

- CRL: http://pki.cleverbase.com/cleverbase3c.crl
- OCSP: http://pki.cleverbase.com/ocsp/3c

The TSP uses both a CRL and the OCSP protocol.

Certificates are included in the CRL until their initial validity has expired. Under normal circumstances, response time is ten seconds or less.

The OCSP protocol is supported using the POST method. Under normal circumstances, response time is ten seconds or less. As a minimum, the OCSP response is always as up-to-date as the CRL, because it is updated real-time. The OCSP response is positive if and only if the TSP's administration confirms that the certificate was issued by the TSP and is still valid. The OCSP service supplies information on the certificate validity until at least six months after its expiration.

In case of a difference in CRL and OCSP response (for instance, when the CRL nears its update interval), the OCSP response prevails.

In the circumstance of a CA key compromise, the OCSP service will continue to be available.

4.10.2 Service Availability

The electronic repository is available 24 hours a day and 7 days a week.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

After expiration of a certificate's validity, the TSP invites the subscriber to renew the certificate. If the certificate is not renewed (timely), the agreement between the TSP and the subscriber ends as of right. The certificate expires automatically. The TSP retains the data regarding the certificate for another seven years.

If a certificate is revoked based on section 4.9, and the subscriber does not apply for a new certificate, the agreement between the TSP and the subscriber ends as of right. The TSP retains the data regarding the certificate for another seven years.

4.12 Key Escrow and Recovery

The TSP does not support key escrow.

4.12.1 Key Escrow and Recovery Policy and Practices

The TSP does not support key escrow.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The TSP does not support key escrow.

5 Facility, Management and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Cleverbase has multiple physical sites:

The Hague site
The TSP is based in a shared office building in The Hague. This office has a lockable door, the keycards of which are kept by Cleverbase.

Delft and Rotterdam sites
The TSP's data centers are based in Rotterdam and Delft and are administered by one and the same external party and are secured in the same way.

The data centers are guarded 24/7. All rooms in the datacenter have CCTV observation. Visitors must identify themselves and are escorted to their destinations. All visits are logged. The cabinet containing the equipment owned by the TSP is used exclusively by the TSP and is lockable.

Within the datacenter, controls are in place to ensure security in emergencies. For use during power outings, an emergency power unit is available, which is tested at least once every three months. A climate control system ensures stable air supply, temperature, and air humidity. The rooms are equipped with moisture detection sensors. A sophisticated fire extinction system is installed.

Storage is redundant by default with copies distributed over two different data centers as a minimum. Storage media that are no longer in use will be destroyed.

5.1.2 Physical Access

Please refer to section 5.1.1.

5.1.3 Power and Air Conditioning

Please refer to section 5.1.1.

5.1.4 Water Exposures

Please refer to section 5.1.1.

5.1.5 Fire Prevention and Protection

Please refer to section 5.1.1.

5.1.6 Media Storage

Media is stored in on-site safes.

5.1.7 Waste Disposal

Adequate measures are taken to dispose of sensitive information.

5.1.8 Off-site Backup

No stipulation.

5.2 Procedural Controls

5.2.1 Trusted Roles

The TSP's staff members are assigned various trusted roles with corresponding responsibilities. Their authorizations correspond to their roles. Roles include:

1. Security officers: overseeing that established security guidelines are implemented and observed.
2. System auditors: having a supervising role and assessing independently how business processes are arranged/organised and to what extent reliability requirements are met.
3. System administrators: administering the TSP systems, including installation, configuration, and maintenance of the systems.
4. System operators: responsible for the daily management of the TSP-systems.
5. Registration officers: responsible for performing the registration process and for manually processing revocation requests.

5.2.2 Number of Persons Required per Task

At least two people are needed for the registration officer and system administrator task.

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.2.4 Roles Requiring Separation of Duties

Registration Officers. For each certificate application, duties are separated between a handling registration officer and an approving registration officer.

System administrators. For each operation on Cleverbase TSP systems two system administrators are required to execute these operations.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Organisation members are screened before entering into service with the TSP, involving, as a minimum, a request for a Certificate of Conduct. Each employee's resume and compulsory identity document are verified. Screening intensity is adjusted to the confidentiality level linked to the employee's role. All organisation members sign a nondisclosure agreement as part of their employment contract.

5.3.2 Background Check Procedures

Please refer to section 5.3.1.

5.3.3 Training Requirements

Organisation members have sufficient knowledge and expertise to fulfil their tasks within the TSP. In particular, the TSP ensures that they are trained in TSP-specific procedures.

5.3.4 Retraining Frequency and Requirements

Regular retraining is performed for the TSP roles.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorised Actions

Unpermitted actions by organisation members may entail disciplinary measures by the TSP's management.

5.3.7 Independent Contractor Requirements

Contractors are subject to the same requirements described in section 5.3.1.

5.3.8 Documentation Supplied to Personnel

The TSP provides the personnel with the documentation required in order to perform the TSP roles.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The TSP records various events for periodic audit purposes:

- CA key life-cycle events:
  - Generation, backup, storage, recovery, archiving and destruction of the CA key
- Certificate life-cycle events:
  - Preparation of the Ubiqu token or preparation of keys in Vidua TW4S system
  - Registration of the certificate holder, subscriber, certificate manager, and certificate coordinator
  - Certificate generation
  - Certificate revocation
  - Certificate acceptance and rejection
  - Generation of the CRL and OCSP entries
- System events:
  - Software installations, updates or removal
  - Installation or removal of storage media
  - Access to the physically secured room housing the systems
  - Hardware security module (HSM) installation, updates, or removal
- Events involving:
  - Routers, firewalls, and network system components
  - Database activities and events
  - Transactions
  - Operating systems
  - Access control systems
  - Mail servers
  - Successful and unsuccessful attacks on PKI systems
  - Activities of staff in PKI systems
  - System failure, hardware failure and other irregularities
  - Firewall and router activities
  - Physical entry to and exit from the CA room
  - Reading, writing and deleting data
  - Profile modifications

The following data are included in the audit log, if applicable:

- Source IP address
- Target IP address
- Date and time
- User ID
- Name and description of the event

5.4.2 Frequency of Processing Log

Audit logs are processed following previously mentioned events. Logs are provided with a timestamp using a clock that is synchronised at least once a day with a trusted time source.

5.4.3 Retention Period for Audit Log

Audit logs are stored and accessible for ten years.

5.4.4 Protection of Audit Log

Any interested party (including, as a minimum, the auditor) can request the logs with the TSP. The management supplies the logs, unless this is against third parties' interests, or unless disproportionate technical effort is required.

Logs are stored in more than one location, in such a way that they are accessible for ten years. During this period their integrity is ensured, so that any deletion or modification of records will be noticed. This includes extensive backup and recovery procedures.

5.4.5 Audit Log Backup Procedures

Please refer to section 5.4.4.

5.4.6 Audit Collection System (Internal vs. External)

Please refer to section 5.4.4.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

The audit log and components supporting the audit log are in scope of the TSP's vulnerability management policy and procedures.

5.5 Records Archival

5.5.1 Types of Records Archived

All data that can be relevant for the compliance audit is archived. As a minimum, this data includes: data collected during identification, the certificate life-cycle, and private key usage. Data subject to archiving may be collected from audit logs, databases or in physical documents. These are all archived appropriately. Private keys are not archived.

5.5.2 Retention Period for Archive

Archives are retained for ten years.

5.5.3 Protection of Archive

Archives are secured against unauthorised access and are, as a rule, accessible only for management and internal and external auditors. These may, however, grant access to (part) of the archives to others, if, and only if, those others need this for their tasks.

Archives are secured against modification and deletion. To this end, both organisational and technical controls are in place. Archives are also protected against storage media deterioration. The archives are stored on monitored, redundant hard disks (at least N+1).

5.5.4 Archive Backup Procedures

The entire archive is backed up off-site.

5.5.5 Requirements for Time-stamping of Records

Records are provided with a timestamp using a clock that is synchronised at least once a day.

5.5.6 Archive Collection System (Internal or External)

Please refer to section 5.5.3 and 5.5.4.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

The CA key has a validity term established by the policy authority of PKIoverheid. As soon as the expiration date is less than three years away, a new CA key is installed. From that moment onwards, the old key is no longer used for signing certificates, but only for signing CRLs. As soon as all certificates that were signed with the old key have expired, it will be destroyed.

5.7 Compromise and Disaster Recovery

The TSP has processes in place for handling calamities. A calamity is a situation in which the integrity of certificates is impaired by a cause within the TSP's sphere of influence. Such situations include, among others:

- Compromise of the CA key
- Large-scale compromise of integrity or confidentiality of user data
- Service unavailability considerably exceeds service level agreements

5.7.1 Incident and Compromise Handling Procedures

The TSP has processes in place for handling (security) incidents.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

No stipulation.

5.7.3 Entity Private Key Compromise Procedures

No stipulation.

5.7.4 Business Continuity Capabilities After a Disaster

The TSP has a Business Continuity Plan in place describing the measures to prevent a disruptive incident or disaster from occurring. If such an event were to take place, the measures and services to return to the default situation are described.

5.8 CA or RA Termination

Should the TSP decide to terminate its activities, the termination plan becomes effective, ensuring that termination proceeds in a controlled way. As a minimum, the plan provides measures to inform the supervisors (Rijksinspectie Digitale Infrastructuur and Logius), subjects, suppliers and other parties involved; to ensure certificate revocation remains possible for as long as unrevoked certificates are in use; and to sustain the certificate status service for as long as is minimally required. No last CRL will be issued until all certificates in its scope are either expired or revoked. All data collected by the TSP for registration purposes will be archived in such a way that its confidentiality remains ensured, and that continues to enable the necessary retrieval of records.

At termination the TSP will try to transfer the service provision to another TSP, in order to minimise inconveniences for end users.

The termination plan is revised annually.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The CA key pair
The key pair of the CA is generated in a cryptographic module (HSM) belonging to the CA. The public part of the CA key is physically transferred to the root CA in the form of a certificate signing request (PKCS#10), on the basis of which the root CA generates the certificate. The HSM is configured in such a way that the CA private key can be used exclusively by someone who can prove to be in control of the private key of a registration officer.

The personal certificate key pair
The key pair of personal certificate in case of Ubiqu is generated in FIPS 140-2 level 3 certified HSM. In case of Cleverbase own TW4S system, it is generated inside the EN 419 221-5 certified HSM. Certificate holders can exert remote control of their key pair by using Authenticate or Vidua app on their phone. The certificate holder must also determine a PIN.

The public part of the key of a personal certificate is presented to the CA in the form of a certificate signing request, on the basis of which the HSM signs the certificate. This procedure is executed in the secured environment of the TSP's datacenter.

Key usage is in accordance with the certificate profile, as described in Chapter 7.

6.1.2 Private Key Delivery to Subscriber

Please refer to section 6.1.1.

6.1.3 Public Key Delivery to Certificate Issuer

Please refer to section 6.1.1.

6.1.4 CA Public Key Delivery to Relying Parties

The Cleverbase CA public key is published through the TSP Dissemination Service.

6.1.5 Key Sizes

The TSP CA uses a key length of 2048 or 4096 and cryptographic algorithm SHA256 with RSA encryption.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Key usage is in accordance with the certificate profile, as described in Chapter 7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The CA private key are generated within a Cryptographic Module that meets the requirements identified in FIPS 140-2 level 3 certified HSM.

The subject private keys in case of Ubiqu are generated in FIPS 140-2 level 3 certified HSM. In case of Cleverbase own TW4S system, subject key pairs are generated in EN 419 221-5 certified device and usage is enforced using EN 419 241-2 certified SAM.

The certification status of the Cryptographic Module is actively monitored. In the case of modification of the status, the necessary actions will be taken to ensure the Cryptographic Module in use meets the applicable requirements.

6.2.2 Private Key (n out of m) Multi-person Control

All operations performed on the cryptographic module are under dual control.

6.2.3 Private Key Escrow

The TSP does not support key escrow.

6.2.4 Private Key Backup

The CA private key is backed up by authorised personnel within strict procedures onto multiple smart cards which are stored in a safe.

6.2.5 Private Key Archival

The TSP does not support private key archival.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Please refer to section 6.2.4.

6.2.7 Private Key Storage on Cryptographic Module

Please refer to section 6.2.8.

6.2.8 Method of Activating Private Key

As private keys are stored in a trustworthy system supporting server signing (TW4S), their protection is ensured.

In case of Ubiqu, the end user keys can be used in the FIPS 140-2 level 3 certified HSM, which is configured in such a way that usage is only possible after users enter their PIN in the Authenticate app provided by Ubiqu. An IT audit statement was issued to this effect.

In case of Cleverbase own TW4S system, the private keys are generated inside a CEN EN 419 221-5 certified HSM device. The private keys activation in ensured by CEN EN 419 241-2 certified SAM device. The SIC mobile app generates SAD based on PIN and sends to SAM for private key activation using SAP.

6.2.9 Method of Deactivating Private Key

No stipulation.

6.2.10 Method of Destroying Private Key

No stipulation.

6.2.11 Cryptographic Module Rating

Please refer to section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys are available to the subject via the TSP's user portal and archived for ten years.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificates can never be valid for a longer time period than their parent root certificate. However, it is Cleverbase's policy to renew root certificates as soon as their expiration date is less than three years away, ensuring a minimum validity of three years for end user certificates.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

As private keys are stored in a trustworthy system supporting server signing (TW4S), their protection is ensured. The end user keys can be used in the HSM, which is configured in such a way that usage is only possible after users enter their PIN in a mobile App. Vidua provides two possible mobile apps to operate the end user key. Primarily the Vidua mobile app provided to the end user by Vidua, secondarily the Authenticate app provided by Ubiqu.

6.4.2 Activation Data Protection

Please refer to section 6.4.1.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The TSP has a great number of security controls (based on the TSPs security policies) in place

- Two-factor authentication for systems,
- Cryptographically secured connections,
- Cryptographically secured audit logs
- Separation in development, acceptance and production environments
- Network zoning, physical and logical access control, hardening of systems
- Risk based logging, monitoring and alerting implemented
- Trusted roles assigned and training for operating these systems
- Security assessments; including vulnerability scanning and penetration testing

With significant changes or at least once per year, the configuration of the security controls of the TSP systems and compliance to the TSP security policies is assessed based on a risk assessment.

Taken together, these security controls ensure that the systems used by TSP can be considered 'trustworthy systems' as meant in CEN/TS 419261. An IT audit statement was issued to this effect. Furthermore the security processes comply with the specific requirements in ETSI 319 411-1, ETSI 319 411-2 and ISO27001. Cleverbase is certified against these standards by BSI Group The Netherlands B.V.

6.5.2 Computer Security Rating

Please refer to section 6.5.1.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

Please refer to section 6.5.1.

6.6.2 Security Management Controls

Please refer to section 6.5.1.

6.6.3 Life Cycle Security Controls

Please refer to section 6.5.1.

6.7 Network Security Controls

Please refer to section 6.5.1.

6.8 Time-stamping

Please refer to section 5.4.2.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The Citizen Domain certificate has the following profile:

field		critical	Citizen (G3) Domain (3c)
The Citizen Domain certificate has the following profile:Version			2 (version 3)
SerialNumber			[number unique to the CA, including at least 64 bits of unpredictable random data created by a Cryptographically Secure Pseudo Random Number Generator]
Signature			Sha-256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer*	commonName (2.5.4.3)		Cleverbase ID PKIoverheid Burger CA - G3
	organizationIdentifier (2.5.4.97)		NTRNL-67419925
	organizationName (2.5.4.10)		Cleverbase ID B.V.
	countryName (2.5.4.6)		NL
Validity	notBefore		[date of issue] *(Time stamps mentioned here may deviate a few minutes, cf. RFC 4270, [section 5.1])*
	notAfter		[date of issue + 1095 days] *(Certificates can never be valid for a longer time period than their parent root certificate. However, it is Cleverbase's policy to renew root certificates as soon as their expiration date is less than three years away, ensuring a minimum validity of three years for end user certificates.)*
Subject*	serialNumber		See [section 3.1] Cleverbase does not apply size limits to the givenName and surName attributes; the total number of characters of both attributes is limited to 64 characters. This limit is also applied to the commonName attribute.
	commonName		
	countryName		
	givenName		
	surName		
subjectPublicKeyInfo	algorithm		rsaEncryption (1.2.840.113549.1.1.1)
	subjectPublicKey		[certificate holder's public key]
authorityKeyIdentifier (2.5.29.35)	keyIdentifier	No	[sha1 hash of CA's public key]
subjectKeyIdentifier (2.5.29.14)	keyIdentifier	No	[sha1 hash of the public key in the certificate]
keyUsage (2.5.29.15)		Yes	*Authenticity certificate:* digitalSignature (1000 0000 0) *Encryption certificate:* keyEncipherment dataEncipherment (0011 0000 0) *Non-repudiation certificate:* nonRepudiation (0100 0000 0)

field		critical	Citizen (G3) Domain (3c)
certificatePolicies (2.5.29.32)	policyIdentifier	No	*Authenticity certificate:* 2.16.528.1.1003.1.2.3.1 *Encryption certificate:* 2.16.528.1.1003.1.2.3.3 *Non-repudiation certificate:* 2.16.528.1.1003.1.2.3.2
	cPSuri (1.3.6.1.5.5.7.2.1)		https://pki.cleverbase.com/cps.pdf
	userNotice (1.3.6.1.5.5.7.2.2)		Reliance on this certificate by any party assumes acceptance of the relevant Cleverbase Certification Practice Statement and other documents in the Cleverbase repository.
subjectAltName (2.5.29.17)	otherName	No	MS UPN: [Subject.serialNumber]@2.16.528.1.1003.1.3.3.4.1
CRLDistributionPoints (2.5.29.31)	FullName	No	http://pki.cleverbase.com/cleverbase3c.crl
ExtKeyUsage (2.5.29.37)		No	*Authenticity certificate:* clientAuthentication (1.3.6.1.5.5.7.3.2) documentSigning (1.3.6.1.4.1.311.10.3.12) emailProtection (1.3.6.1.5.5.7.3.4) *Encryption certificate:* emailProtection (1.3.6.1.5.5.7.3.4) encryptingFileSystem (1.3.6.1.4.1.311.10.3.4) *Non-repudiation certificate:* documentSigning (1.3.6.1.4.1.311.10.3.12) emailProtection (1.3.6.1.5.5.7.3.4)
authorityInfoAccess (1.3.6.1.5.5.7.1.1)		No	AccessMethod: id-ad-ocsp (1.3.6.1.5.5.7.48.1) AccessLocation: http://pki.cleverbase.com/ocsp/3c AccessMethod: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) AccessLocation: http://pki.cleverbase.com/CleverbaseBurgerG3.cer
QcStatement (1.3.6.1.5.5.7.1.3)		No	*Only for the non-repudiation certificate:* id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qct-esign (0.4.0.1862.1.6.1) id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (0.4.0.1862.1.5) PDS URL = https://pki.cleverbase.com/pki-disclosure-statement.pdf PDS Lang = en

7.2 CRL Profile

The Cleverbase CRL has the following profile:

field		critical	contents
Version			1 (version 2)
Signature			sha-256WithRSAEncryption
Issuer*	commonName (2.5.4.3)		Cleverbase ID PKIoverheid Burger CA - G3
	organizationIdentifier (2.5.4.97)		NTRNL-67419925
	organizationName (2.5.4.10)		Cleverbase ID B.V.
	countryName (2.5.4.6)		NL
ThisUpdate			[time of issue of the CRL]
NextUpdate			[time of issue of the CRL + 24 hours]
revokedCertificates			[revoked certificates]
CRLNumber (2.5.29.20)		No	[subsequent number]
AuthorityKeyIdentifier (2.5.29.35)		No	[sha1 hash of Cleverbase Organisatie Persoon CA public key]

7.3 OCSP Profile

The Cleverbase OCSP has the following profile:

field		critical	Citizen (G3) Domain (3c)
Version			2 (version 3)
SerialNumber			[number unique to the CA, including at least 8 bytes of unique data]
Signature			Sha-256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer*	commonName (2.5.4.3)		Cleverbase ID PKIoverheid Burger CA - G3
	organizationIdentifier (2.5.4.97)		NTRNL-67419925
	organizationName (2.5.4.10)		Cleverbase ID B.V.
	countryName (2.5.4.6)		NL
Validity	notBefore		[date of issue]
	notAfter		[date of issue + 397 days]
Subject*	commonName (2.5.4.3)		OCSP Signing Cleverbase ID Burger CA - G3
	organizationIdentifier (2.5.4.97)		NTRNL-67419925
	organizationName (2.5.4.10)		Cleverbase ID B.V.
	countryName (2.5.4.6)		NL
subjectPublicKeyInfo	algorithm	No	rsaEncryption (1.2.840.113549.1.1.1)
	subjectPublicKey		Contains the public key
authorityKeyIdentifier (2.5.29.35)	keyIdentifier	No	[sha1 hash of the CA's public key]
SubjectKeyIdentifier (2.5.29.14)	keyIdentifier	No	[sha1 hash of the public key in the certificate]
KeyUsage (2.5.29.15)		Yes	digitalSignature (1000 0000 0)
CertificatePolicies (2.5.29.32)	policyIdentifier	No	2.16.528.1.1003.1.2.3.1
	cPSuri (1.3.6.1.5.5.7.2.1)		https://pki.cleverbase.com/cps.pdf
	userNotice (1.3.6.1.5.5.7.2.2)		Reliance on this certificate by any party assumes acceptance of the relevant Cleverbase Certification Practice Statement and other documents in the Cleverbase repository.
CRLDistributionPoints (2.5.29.31)	FullName	No	http://pki.cleverbase.com/cleverbase3c.crl
ExtKeyUsage (2.5.29.37)		Yes	id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9)
OCSPNoCheck (1.3.6.1.5.5.7.48.1.5)		No	
authorityInfoAccess (1.3.6.1.5.5.7.1.1)		No	AccessMethod: id-ad-calssuers (1.3.6.1.5.5.7.48.2) AccessLocation: [http://pki.cleverbase.com/CleverbaseBurgerG3.cer] (http://pki.cleverbase.com/CleverbaseBurgerG3.cer)

* In accordance with RFC 4514, the order in which distinguished names in this CPS are represented is an inversion of their occurrence in the underlying ASN.1 structure.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

Cleverbase is a trust service provider as meant in the eidas regulation (EU 910/2014). For this reason, it is subject to supervision by the Rijksinspectie Digitale Infrastructuur. Compliance certificates have a validity of two years, with annual interim audits. Moreover, internal audits are performed regularly.

8.2 Identity/Qualifications of Assessor

Cleverbase is certified against the ETSI EN 319 411-1 and ETSI EN 319 411-2 standards by BSI Group The Netherlands B.V., which is in accordance with the ETSI EN 319 403 scheme by an accreditation body within the meaning of Article 4 of Regulation (EC) No 765/200.

8.3 Assessor's Relationship to Assessed Entity

The external auditor performing the compliance audit functions independently from Cleverbase.

8.4 Topics Covered by Assessment

The scope of the compliance audit comprises the following services:

- Registration service
- Certificate generation service
- Revocation management service
- Revocation status service
- Dissemination service
- Subject device provision service
- Remote qualified electronic signatures (QES) service

8.5 Actions Taken as a Result of Deficiency

If, unexpectedly, deviations are found, a Corrective Action Plan is drafted to correct the deviations. The Corrective Action Plan is agreed upon with the external auditor and is given to the disposal of the Rijksinspectie Digitale Infrastructuur and the Policy Authority Logius.

8.6 Communication of Results

Compliance audit certificates can be consulted on Cleverbase's website: https://vidua.nl/legal/qualifications/. The underlying audit reports are confidential, and are confidentialy shared wiht the Rijksinspectie Digitale Infrastructuur and the Policy Authority Logius.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Certificate issuance may be either charged or free of charge. The TSP enters into detailed agreements with subscribers for single or periodic payments.

9.1.2 Certificate Access Fees

No compensation is required for the provision of certificate status information or other information on certificates. Only if exceptional efforts are required to answer an information request, reasonable costs can be charged. In such a case, the requester of this information is informed about the costs before committing to any expenditures.

9.1.3 Revocation or Status Information Access Fees

Please refer to section 9.1.2.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The TSP shall not be liable for any damage caused by the TSP, unless in cases and insofar as described in art. 13 of the eidas regulation. The TSP's general terms and conditions contain the same limitation of liability. In order to cover this liability, the TSP has arranged liability insurance covering up to at least 2,500,000.- euro.

The TSP is not liable if certificates are not used as described in the certificates themselves.

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

The TSP considers all data provided within the framework of the certification service as confidential.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

Any party having confidential information at its disposal is responsible for ensuring its confidentiality.

9.4 Privacy of Personal Information

The TSP has an Information Security Management System (ISMS) in place, ensuring confidentiality of personal data processed by the TSP. Furthermore the TSP's Privacy Statement is applicable to all the provided services.

9.4.1 Privacy Plan

Please refer to the Cleverbase Privacy Statement available on the public website.

9.4.2 Information Treated as Private

Please refer to the Cleverbase Privacy Statement available on the public website.

9.4.3 Information Not Deemed Private

Please refer to the Cleverbase Privacy Statement available on the public website.

9.4.4 Responsibility to Protect Private Information

Please refer to the Cleverbase Privacy Statement available on the public website.

9.4.5 Notice and Consent to Use Private Information

Please refer to the Cleverbase Privacy Statement available on the public website.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Please refer to the Cleverbase Privacy Statement available on the public website.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

All documents, products and services made public by the TSP are subject to the TSP's copyright and/or it's suppliers/licenses. It must be stressed here that this does not apply to documents that are signed by certificate holders using a TSP-issued certificate. The TSP indemnifies clients against claims by third parties regarding possible violations of intellectual property rights by the TSP.

9.6 Representations and Warranties

The TSP hereby warrants that it:

1. observes the procedures described in this CPS;
2. has performed all reasonable actions in order to ensure that information included in the issued certificates is correct at the time of issuance;
3. will revoke certificates if it presumes that data in the certificates is not or no longer accurate, or that the private key correlating to the certificate was compromised.

9.6.1 CA Representations and Warranties

No stipulation, please refer to section 9.6.

9.6.2 RA Representations and Warranties

No stipulation, please refer to section 9.6.

9.6.3 Subscriber Representations and Warranties

No stipulation, please refer to section 9.6.

9.6.4 Relying Party Representations and Warranties

No stipulation, please refer to section 9.6.

9.6.5 Representations and Warranties of Other Participants

No stipulation, please refer to section 9.6.

9.7 Disclaimers of Warranties

No limitations of warranties apply other than those mentioned in section 9.6.

9.8 Limitations of Liability

No limitations of liability apply other than those mentioned in section 9.2.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

The TSP's CPS becomes effective immediately after publication in the public repository and remains effective until a new version is published.

9.10.2 Termination

No stipulation.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 Individual Notices and Communications With Participants

The TSP can be contacted via mail, electronic mail and telephone. The TSP publishes information on its public website and contacts individual subjects via electronic mail or telephone.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CPS are made using the pre-defined, regular procedures for changing components of the TSP services.

9.12.2 Notification Mechanism and Period

Please refer to section 9.10.1.

9.12.3 Circumstances Under Which OID Must Be Changed

No stipulation.

9.13 Dispute Resolution Provisions

If a dispute arises between the TSP and a customer, or between the TSP and a third party, the TSP's management, having heard all involved and considered all interests at stake, decides. Such a decision is written down and delivered within a reasonable period of time. This procedure does not limit the possibility to submit disputes to the civil court in The Hague.

9.14 Governing Law

All the TSP's activities are subject to Dutch law.

9.15 Compliance With Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

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.

9.17 Other Provisions

No stipulation.

Annex: Issuing Certificates Fingerprints

Cleverbase ID PKIoverheid Burger CA - G3. Fingerprint: de0a92e5435b613208dc435ecc7158bf28f420a93e0a91d5965972053f523549 N=Cleverbase ID PKIoverheid Burger CA - G3, OID.2.5.4.97=NTRNL-67419925, O=Cleverbase ID B.V., C=NL