Certification Practice Statement

NOTE: This is the official version of the Cleverbase Certificate Practice Statement. For convenience, a non-official Dutch version is also available on the Cleverbase website.

Table of contents

Document control

Version history

Version	Date	By	Amendments
0.1	15-03-2017	Vincent de Haan	Initial edition
1.0	21-04-2017	Vincent de Haan	Final version
1.1	20-07-2017	Vincent de Haan	Minor changes
1.2	28-08-2017	Vincent de Haan	Changes in CPS, CRL, OCSP addresses; minor changes in section 5.1.2, authorityInfoAccess included in certificate profile, minor changes in section 9.2
1.3	2-09-2017	Vincent de Haan	Minor changes to the certificate profiles
1.4	09-11-2017	René Kleizen	Correction of CRL and OCSP URLs and PublicKeyInfo algorithm
1.5	13-3-2018	Vincent de Haan	Address change, linguistic changes, specification of certificate profiles, English translation
1.6.0	12-4-2018	Vincent de Haan	Change of field authorityInfoAccess in end user profile
1.7.0	14-06-2018	Raúl Maduro	Changed incorrect link to https://pki.cleverbase.com/pki-disclosure-statement.pdf Added support of Dutch ID cards, minor change to opening hours customer service and other minor linguistic changes

1. Introduction

1.1 Overview

PKIoverheid is a *public key infrastructure* (PKI) set up at the initiative of the Dutch government, to be used for electronic signatures, electronic authentication, and confidential electronic communication, and adjusted to relevant Dutch and European legislation. Certificates issued within this PKI are highly reliable. Several trust service providers (TSPs) are active in this PKI and are trusted to issue certificates. Root certificates in this PKI are signed by the State of the Netherlands.

Cleverbase acts as a TSP in PKIoverheid, aiming at providing both citizens and businesses with the certificates they need to exchange, reliably and confidentially, information with each other and the government. As a rule, certificate holders register remotely by way of a video call using a mobile app to have their identities and identity documents verified, after which Cleverbase issues the certificates they apply for.

The key material belonging to the certificate is stored in a trustworthy system for server signing (TW4S): the private keys of the end user certificates are stored in a hardware security module (HSM) in Cleverbase's datacenter, which is configured in such a way that certificate holders hold exclusive control of their keys. They exert this control using an app that is linked to their mobile phone and a PIN of their own choosing. The TW4S is administered by Ubiqu B.V.

1.2 Document properties

This document is Cleverbase's Certification Practice Statement. It is based on the Statement of Requirement PKIoverheid[1], ETSI EN 319 411-1, ETSI EN 319 411-2[2] and the eidas regulation[3]. Its layout is modeled after RFC 3647.

This CPS covers issuance of certificates to the 'persoon burger' target group governed by the certificate policy (CP) as stated in section 3c of the Statement of Requirement PKIoverheid. It supports the usage purposes of authenticity, non-repudiation and encryption. For each combination of target group and usage purpose a separate OID is defined in the relevant CP. An overview follows:

	authenticity	non-repudiation	encryption*
'persoon burger' (section 3c SoR)	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 Participants

The following participants in PKIoverheid are relevant here:

Policy authority (PA). The policy authority's task is to administer the entire system of agreements and to regulate the required supervision. Logius fulfills this task on behalf of the State of the Netherlands.

Cleverbase. Cleverbase ID B.V., registered at the Chamber of Commerce under number 67419925.

---

[1] Available at https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-tsp/programma-van-eisen/

[2] Both available at http://www.etsi.org/standards

[3] http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32014R0910

Cleverbase CA. Cleverbase's certification authority is responsible for issuing certificates.

Cleverbase RA. Cleverbase's registration authority is responsible for establishing the identity of prospective holders of certificates to be issued by Cleverbase. Staff members of the registration authority are called registration officers.

Certificate holder. The certificate holder is the entity stated in the subject field of the certificate, and the holder of the private key. Holders of personal certificates are natural persons. Holders of certificates in the 'Burger' domain are also subscribers.

Subscriber. Holders of certificates in the 'Burger' domain are themselves subscribers. In the case of a certificate in the 'Organisatie' domain, the organization for which the certificate is issued is the subscriber.

Relying party. A relying party is anyone who acts trusting a certificate issued by Cleverbase.

Ubiqu. Ubiqu Access B.V. supplies Ubiqu tokens to be issued to personal certificate holders. These tokens consist of two parts: a set of private keys stored on a TSP-administered server, and an app on the certificate holder's mobile phone. Using this app, certificate holders can exert exclusive control of their private keys. Although Ubiqu administers this server, Cleverbase is the principal responsible for its administration. Certificate holders have exclusive control of their tokens, to be exerted using their mobile phone and PIN.

1.4 Certificate usage

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 of the 'persoon burger' type may be used by individual natural persons in private, i.e., not in business contexts.

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 usage purposes correspond to the keyUsage field in the certificate.

	authenticity	encryption	signature
'persoon burger' (section 3c SoR)	digitalSignature	keyEncipherment dataEncipherment keyAgreement	nonRepudiation

1.5 Administration of this CPS

Cleverbase assesses this CPS and corrects any errors or omissions twice a year, as well as each time the policy authority issues a new version of the Statement of Requirement. The TSP publishes any intended amendments to this CPS on its web site in due time, after which the TSP's management eventually establishes the CPS.

Please address any enquiries or other communications to:

info@cleverbase.com

Or, alternatively, to:

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

2 Publication and repository responsibilities

2.1 Electronic repository

Cleverbase has an electronic repository, accessible through www.cleverbase.com. The *certificate revocation list* (CRL) and the OCSP server are available at:

CRL: http://pki.cleverbase.com/cleverbase3c.crl

OCSP: http://pki.cleverbase.com/ocsp/3c

As a rule, the electronic repository is accessible at any time. In the case of (planned) maintenance or a calamity, accessibility can be interrupted for a maximum of four hours.

The electronic repository is secured against unauthorized modifications. Only the TSP has writing permissions for the electronic repository.

2.2 Publication of TSP information

The following information is accessible in the electronic repository:

- this Certification Practice Statement,
- the general terms and conditions,
- the certificates (end user certificates being accessible for certificate holders only),
- the certificate status service.

Earlier versions of the CPS and the general terms and conditions, including a version history, will be kept available.

3 Identification and authentication

This section describes the identification and authentication processes during initial registration and prolongation. Two registration processes are supported, one involving remote identification and the other a personal meeting. These processes are described separately.

3.1 Naming

The certificate holder is identified in the subject field of the certificate with a *distinguished name* (DN) as meant in X.501. Required DN components differ for various certificate types:

	'persoon burger'
serialNumber	personal number, unique to the CA
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)

The above implies the following, among others:

- Pseudonymous or anonymous certificates are not allowed.
- Each DN is unique.
- Each DN has a meaningful relation to the represented entity.

If opinions on naming differ, the registration authority decides.

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

3.2 Initial identity validation

As a rule, Cleverbase registers natural persons remotely, using a dedicated mobile app. If remote registration turns out to be impossible, registration can take place in a personal meeting.

3.2.1 Remote initial identity validation

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 email address of the user is registered for use as a user name at Cleverbase.
(2) The Authenticate app (part of the Ubiqu token) is installed on the phone. The prospective certificate holder chooses a PIN, and a link is established between PIN, phone, and the (future) identity.
(3) A selfie of the prospective certificate holder is made and sent to the server.
(4) A photo of the prospective certificate holder's Dutch passport or Dutch ID card is made and sent to the server, together with the personal data required for registration. (Prospective certificate holders without a Dutch passport or Dutch ID card cannot apply for a certificate with Cleverbase.)
(5) The app sets up a video connection with a registration officer, who, before and during the video call, performs the following checks:
    (a) The registration officer checks the quality of the video connection and may give instructions regarding ambient light and sound.
    (b) The registration officer checks the data submitted against the picture in the identity document.
    (c) The registration officer verifies authenticity and validity of the identity document, checking, among other things, whether it has been recorded stolen or missing.
    (d) The registration officer checks the identity document's authenticity features.
    (e) The registration officer verifies the prospective certificate holder's identity.
    (f) The registration officer checks whether the applicant has earlier applied for a certificate with Cleverbase. (In this case existing certificates are revoked.)
    (g) The registration officer requests the applicant to read aloud a unique code and to express the unambiguous will to apply for a certificate.
(6) If all checks have positive results, the registration officer approves the certificate application.
(7) A second registration officer checks the certificate application and approves it if s/he finds that all requirements are met.
(8) The certificate holder receives a revocation code by email to be used if s/he decides to revoke the certificate later on.

The TSP has controls in place for 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.
- Applicants with unusual or damaged (although still valid) identity documents, persevering problems in establishing an appropriate video connection, or other peculiarities preventing the process described above from ensuring reliable identification, are invited to have their identities established in a personal meeting at the TSP's premises.

3.2.2 Personal initial identity validation

Users who are unable register remotely, but who have both a phone allowing for installation of the registration app and a Dutch passport or Dutch ID card , can register at Cleverbase in person. In such a case the applicant visits TSP's premises, where a registration officer starts by verifying the applicant's identity and identity document. If s/he decides that the identity can be established and that certificate issuance is possible, the registration process as described in section 3.2.1 is now performed in person, with personal identity validation replacing remote identification. Registration is not possible for users without a suited phone or Dutch passport or Dutch ID card .

3.3 Identification and authentication at certificate renewal

Certificate renewal involves the same procedure as initial certificate application. In this case registration includes revocation of any old certificates that may still be valid.

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 and enter it in the public section of Cleverbase's web site.
- Certificate holders contact Cleverbase by phone and answer a few questions relating to their personal data, by which the registration officer establishes their identity.
- Certificate holders send a letter or email to Cleverbase, enclosing a copy of their identity document.

4 Certificate life-cycle operation requirements

4.1 Certificate application

A description of the application process for each certificate type follows.

4.1.1 Application for a certificate of the 'persoon burger' type

Prospective certificate holders apply for certificates of the 'persoon burger' type. At that moment they close 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.

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 Processing the certificate application

Please refer to section 4.1.

4.3 Certificate issuance

Please refer to section 4.1.

4.4 Certificate acceptance

Certificates of the 'persoon burger' type are accepted by implication.

4.5 Key pair and certificate usage

Any agreement closed with 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 (see section 1.4).

Before trusting a certificate, relying parties should check the following:

(1) certificate usage in accordance with the usage purposes described in the certificate and the general terms and conditions,
(2) the 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.

4.6 Certificate renewal

Certificate renewal without changing key pairs is not supported. A renewal is processed as a new application.

4.7 Certificate re-key

If a certificate holder applies for a new certificate with a new key pair, the same procedures are followed as during initial certificate application. Any changes in terms or conditions resulting from interim reviews are pointed out during application.

4.8 Certificate modification

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

4.9 Certificate revocation and suspension

A certificate can be revoked under circumstances. The TSP will then put it on a *certificate revocation list* (CRL) and announce through the OCSP (Online Certificate Status Protocol) that it was revoked. This section describes under which circumstances, by whom and in which way a certificate can be revoked.

Certificates cannot be revoked or deactivated temporarily.

4.9.1 Circumstances for certificate revocation

A certificate can be revoked under the following circumstances:

(a) The subscriber requests for revocation.

(b) Confidentiality of the private key corresponding to the certificate's public key was presumably impaired. Cases include those in which a mobile phone linked to the Ubiqu token was lost or stolen, or confidentiality of the PIN was impaired.
(c) The certificate holder fails to comply with her/his obligations based on this CPS or the agreement closed with her/him.
(d) Information in the certificate is not or no longer correct and up-to-date, or information in the certificate is misleading.
(e) There are indications that the certificate is misused.
(f) In retrospect, the certificate appears not to have been issued following the proper procedures.
(g) The TSP terminates its activities with no other TSP taking over the CRL and OSCP services.
(h) The policy authority of PKIoverheid determines that the certificate does not meet requirements.
(i) Revoking the certificate can help prevent or fight a calamity.
(j) Other circumstances justify, in the TSP's view, revoking the certificate in order to sustain trust in the public key infrastructure.
(k) The subscriber, who is a natural person, has passed away.

4.9.2 Parties entitled to request certificate revocation

A certificate may be revoked at the initiative of:

(a) the TSP itself,
(b) the certificate holder,
(c) the subscriber.

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

4.10 Certificate revocation procedure

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 for revocation by contacting the TSP's customer service by phone between 9.00 AM and 5.00 PM, or by email out of office hours. For contact data, please refer to the web site, https://cleverbase.com.

In non-urgent situations, revocation requests can also be submitted by mail to the following address:

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

Revocation requests by email or mail must be submitted with a copy of a valid identity document.

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

Revocation is effectuated within four hours after receipt of the request, by putting the certificate on the *certificate revocation list* and updating the OCSP response. After it is established that revocation is necessary, the certificate status is updated within sixty minutes.

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

If the TSP receives information that 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 twenty-four hours, or as fast as possible during business hours.

Certificate holders who themselves revoke certificates by using the web portal or by phone are given feedback as soon as revocation is successful. If a revocation request is submitted by mail, or if someone else than the certificate holder initiates revocation, an email is sent to the certificate holder.

4.11 Certificate status service

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 *certificate revocation list* (CRL) and the OCSP protocol.

The CRL is updated at least once every seven days. 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 *GET 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 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 until at least six months after its expiration.

4.12 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's validity 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 certificate's validity expires because the certificate is put on the *certificate revocation list* as described in section 4.9. The TSP retains the data regarding the certificate for another seven years.

4.13 Key escrow

The TSP does not support key escrow.

5 Management, operational and physical controls

5.1 Physical security controls

5.1.1 The Hague site

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

5.1.2 Delft and Rotterdam sites

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

The datacenters 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 datacenters as a minimum.

Storage media that is no longer in use is destroyed.

5.2 Procedural controls

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

- Security officers: overseeing that established security guidelines are implemented and observed.
- System auditors: having a supervising role and assessing independently how business processes are put in order and how reliability requirements are met.
- System administrators: administering the TSP systems, including install, configuration, and maintenance of the systems.
- System operators: responsible for the daily management of the TSP-systems.
- Registration officers: responsible for performing the registration process and for manually processing revocation requests. For each certificate application, duties are separated between a handling registration officer and an approving registration officer.

5.3 Personnel security controls

Staff members are screened before entering 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.

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

All staff members and hired third persons sign a nondisclosure agreement as part of their employment contract or commission contract, respectively.

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

Reliability of externals performing tasks for the TSP is also investigated.

5.4 Audit logging procedures

The TSP records various events for periodic audit purposes. 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.

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 disproportional technical effort is required.

Logs are provided with a time stamp using a clock that is synchronized at least once a day.

As a minimum, events logged include the following:

- 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
  - 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 install, updates, or uninstall
  - 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

5.5 Records archival

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.

Archives are retained for ten years.

Archives are secured against unauthorized access and are, as a rule, accessible only for the 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 organizational 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).

The entire archive is backed up off-site.

5.6 CA 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 and OCSP responses. As soon as all certificates that were signed with the old key have expired, it will be destroyed.

5.7 Calamities

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

- Unauthorized access to the CA key
- Both datacenters are inaccessible
- The Ubiqu token provider is inaccessible

5.8 CA 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 for measures to inform all parties involved, to sustain the certificate status service, and to keep certificate revocation possible as long as unrevoked certificates are in use. All data collected by the TSP for registration purposes will be archived in such a way that both its confidentiality and its accessibility for required consult are ensured.

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

The termination plan is updated annually.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 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 key pair can be used exclusively by someone who can prove to be in control of the personal key pair of a registration officer.

6.1.2 The personal certificate key pair

The key pair of personal certificates is generated in a cryptographic module (HSM) in the TSP's datacenter. Certificate holders can exert remote control of their key pair by using an app on their phone.

During certificate application the app is linked to the phone by way of an identifying number of the 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.

6.2 Private key protection

As private keys never leave the cryptographic hardware, their protection is ensured. End user keys are contained in an HSM configured in such a way that they can be used only after users enter their PIN in the Authenticate app provided by Ubiqu.

6.3 Activation data

Activation data have a role in the TSP's internal processes only and, therefore, need not to be described here.

6.4 System controls

The TSP has a great number of security controls in place (two-factor authentication for systems, cryptographically secured connections, cryptographically secured audit logs, etc.). Taken together, these security controls ensure that the systems used by TSP can be considered 'trustworthy systems' as meant in ETSI EN 419 261. An IT audit statement was issued to this effect.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate profiles

field		critical	'persoon burger' (3c)
Version			2
SerialNumber			[number unique to the CA, including at least 8 bytes of unpredictable random 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][4]

[4] Time stamps mentioned here may deviate a few minutes, cf. RFC 4270, section 5.1.

	notAfter		[date of issue + 1095 days][5]
Subject*	serialNumber		See section 3.1
	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)
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

[5] 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.

	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)		No	AccessMethod: id-ad-ocsp (1.3.6.1.5.5.7.48.1) AccessLocation: http://pki.cleverbase.com/ocsp/3c AccessMethod: id-ad-calssuers (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 profiles

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 + 7 days]
revokedCertificates			[revoked certificates]
CRLNumber		No	[subsequent number]

7.3 OCSP profiles

field		critical	'persoon burger' (3c)
Version			2
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 + 1095 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.
subjectAltName (2.5.29.17)	otherName	No	Microsoft UPN: 42@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	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)		No	AccessMethod: id-ad-ocsp (1.3.6.1.5.5.7.48.1) AccessLocation: http://pki.cleverbase.com/ocsp/3c

* 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

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 Radiocommunications Agency Netherlands (Agentschap Telecom).

Cleverbase was certified against the ETSI EN 319 411-1 and ETSI EN 319 411-2 norms by BSI Group The Netherlands B.V., which in turn was certified by UKAS. At certification a statement was delivered implying that Cleverbase issues certificates in accordance with part 3c of the Statement of Requirement PKIoverheid and the eidas regulation. The auditor performing the compliance audit has no relationship whatsoever with Cleverbase.

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

Compliance certificates have a validity of two years, with annual interim audits. Moreover, internal audits are performed regularly.

If, unexpectedly, deviations are found, a plan is drafted to correct them at short notice.

Compliance audit certificates can be consulted on Cleverbase's web site. The underlying audit reports are confidential, but are put at the disposal of the Radiocommunications Agency Netherlands (Agentschap Telecom).

9 Other business and legal matters

9.1 Fees

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

No reimbursement 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.

9.2 Financial responsibilities

The TSP shall not be liable for any damage caused by the TSP, unless in cases and to the extent as described in art. 13 of the eidas regulation. The TSP's general terms and conditions contain the same limitation of liability. The TSP is not liable if certificates are not used as described in the certificates themselves.

In order to cover this liability, the TSP has arranged a liability insurance covering up to at least 1,000,000.- euro.

9.3 Confidentiality of business information

The TSP considers all data provided within the framework of the certification service as confidential, except for data in certificates of the 'server organization' type.

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

9.4 Protection of personal data

The TSP has an information security management system (ISMS) in place, ensuring confidentiality of personal data processed by the TSP.

9.5 Intellectual property rights

All documents made public by the TSP are subject to the TSP's copyright. 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 Statements and warranties

The TSP hereby warrants that it:

(a) observes the procedures described in this TPS,
(b) has performed all reasonable actions in order to ensure that information included in the issued certificates is correct at the time of issuance,
(c) will revoke certificates if it presumes that data in the certificates is not or no longer accurate, or that the private key belonging to the certificate was compromised.

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 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.

9.10 Governing law

All TSP's activities are subject to Dutch law.