Kitemark™ Certificate

This is to certify that:

Cleverbase ID B.V.
Maanweg 174
Den Haag
2516 AB
The Netherlands

Holds Certificate Number: ETS 057

In respect of:

Regulation (EU) N° 910/2014
Regulation (EU) No 910/2014 ("eIDAS") ETSI EN 319 411-2 - Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

Delivers Trust Services according to the requirements of the standard mentioned above for services specified (see page with detailed scope).

This issues the right and license to use the Kitemark in accordance with the Kitemark Terms and Conditions governing the use of the Kitemark, as may be updated from the time by BSI Assurance UK Ltd (the "Conditions"). All defined terms in this Certificate shall have the same meaning as in the Conditions..

The use of the Kitemark is authorized in respect of the Trust Services detailed on this Certificate provided at or from the addresses specified on following page(s).

For and on behalf of BSI:

Denelise L'Ecluse, Managing Director Assurance - Continental Europe

First Issued: 2017-11-17
Latest Issue: 2024-09-25

Effective Date: 2024-08-01
Expiry Date: 2026-07-31

Page: 1 of 4

Kitemark™ Certificate

No. ETS 057

On the request of Cleverbase ID B.V. (hereafter referred to as: Cleverbase), the annual recertification audit on all areas and processes and subsequent follow-up audit was performed by BSI Group The Netherlands B.V. (John M. Keynesplein 9, 1066 EP Amsterdam, The Netherlands).

The full audit covered all applicable requirements from the audit criteria listed below (see "Audit Information") and are defined in Cleverbase's Statement of Applicability, dated 1 March 2024 and the Overview of Applicability, version 5.4, dated March 2024.

The scope of the assessment comprised the following Trust Service Provider component services:
-   Registration Service
-   Certificate Generation Service
-   Dissemination Service
-   Revocation Management Service
-   Revocation Status Service
-   Subject Device Provision Service

These TSP component services are being provided for:
-   Issuance of qualified certificates for electronic signatures (qualified trust service), in accordance with the policy: QCP-n-qscd

The certificates are issued through its issuing certification authorities, as specified below:
Root CA: Staat der Nederlanden Root CA - G3 (not in scope)
Domain CA: Staat der Nederlanden Burger CA – G3 (not in scope)
(Active) Issuing CA: CN = Cleverbase ID PKIoverheid Burger CA - G3
-   O = Cleverbase ID B.V.
-   Serialnumber: 7796d55e296d01ccf50cedb3707b0dd842695535
-   Valid from April 17, 2019 to November 12, 2028
-   SHA-256 fingerprint: DE0A92E5435B613208DC435ECC7158BF28F420A93E0A91D5965972053F523549
    +   PKIOverheid Personal Citizen Non-Repudiation (OID 2.16.528.1.1003.1.2.3.2), in accordance with policy QCP-n-qscd

The Certification Authority processes and services are documented in the following documents:
-   Certification Practice Statement Cleverbase ID, version 1.18, dated 11 March 2024
-   PKI Disclosure Statement, version 1.4.1, dated 5-3-2024

First Issued: 2017-11-17
Latest Issue: 2024-09-25

Effective Date: 2024-08-01
Expiry Date: 2026-07-31

Kitemark™ Certificate

No. ETS 057

Our annual recertification audit was performed in April 2024. The result of the full audit is that we conclude, based on the objective evidence collected during the audit, between 15 April 2023 and 14 April 2024, the areas assessed during the audit were generally found to be effective, based on the applicable requirements defined in Cleverbase's Statement of Applicability, dated 1 March 2024 and the Overview of Applicability, version 5.4, dated March 2024.

A point in time audit was performed between 15 and 17 July 2024 to extend the scope of certification with:

- ETSI TS 119 461 V1.1.1 (2021-07) Policy and security requirements for trust service components providing identity proofing of trust service subjects - use cases Hybrid attended remote & Manual attended remote;
- ETSI TS 119 411-6 V1.1.1 (2023-08) Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates. We concluded that standard ETSI TS 119 411-6 is in scope as the CA is technically capable to issue S/MIME certificates. However, the standard is not applicable because the CA does not include an email address (in the form of an rfc822Name or an otherName of type id-on-SmtpUTF8Mailbox) in the subjectAltName extension.

The result of the scope extension audit is that we conclude, based on the objective evidence collected during the audit, from 17 July 2024, the areas assessed during the audit were generally found to be effective, based on the applicable requirements defined in Cleverbase's Statement of Applicability, dated 16 July 2024 and the Overview of Applicability, version 5.7, dated July 2024.

Audit information (period of time):

Audit criteria:

- ETSI EN 319 401 v2.3.1 (2021-05) General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 v1.4.1 (2023-10) Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates – Part 1: General requirements
- ETSI EN 319 411-2 v2.5.1 (2023-10) Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates
- CA/Browser Forum – Network and Certificate System Security Requirements v1.7
- PKIoverheid - Programme of Requirements v4.12 (G3 Legacy Citizen certificates - previously 3c)
- Regulation (EU) N 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Chapter III – Trust Services

Audit Period of Time:

15 April 2023 – 14 April 2024

Audit performed:

April 2024

First Issued: 2017-11-17

Latest Issue: 2024-09-25

Effective Date: 2024-08-01

Expiry Date: 2026-07-31

Kitemark™ Certificate

No. ETS 057

Audit information (point in time):

Audit criteria:

- ETSI TS 119 461 V1.1.1 (2021-07) Policy and security requirements for trust service components providing identity proofing of trust service subjects - use cases Hybrid attended remote & Manual attended remote;
- ETSI TS 119 411-6 V1.1.1 (2023-08) Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates. We concluded that standard ETSI TS 119 411-6 is in scope as the CA is technically capable to issue S/MIME certificates. However, the standard is not applicable because the CA does not include an email address (in the form of an rfc822Name or an otherName of type id-on-SmtpUTF8Mailbox) in the subjectAltName extension.

Audit Point in Time:

17 July 2024

Audit performed:

July 2024

Information and Contact:

BSI Group the Netherlands B.V., John M. Keynesplein 9, 1066 EP Amsterdam, NL

First Issued: 2017-11-17

Latest Issue: 2024-09-25

Effective Date: 2024-08-01

Expiry Date: 2026-07-31