

Audit Attestation <<Name>> <<Number>>

## Audit Attestation for name of the audited company

**Kommentiert [A1]:** Please ensure you follow the requirements stated in section 5.1 Audit Statement Content of <https://www.ccadb.org/policy#51-audit-statement-content>

**Reference: No. unique identifier**

“Place, Issuing date”

**Kommentiert [A2]:** Date the audit statement was written, which will necessarily be after the audit period end date or point-in-time date - see date format specifications below and <https://www.ccadb.org/policy#51-audit-statement-content>:

To whom it may concern,

Only the following date format is accepted according to ETSI TS 119 403-2. This applies to all occurrences of dates throughout the attestation:  
- YYYY-MM-DD example: 2016-05-07

This is to confirm that “CAB name” has audited the CAs of the “name of the audited company” without critical findings.

No extra text within the date, such as “7th” or “the”.  
If used, month names must be in English.

This present Audit Attestation Letter is registered under the unique identifier number “n°” and consists of << 8 >> pages.

**Kommentiert [A3]:** In case the attestation is issued with critical findings, use “with” instead and provide explanation.

Kindly find here below the details accordingly.

In case of any question, please contact:

CAB\_company\_name  
street  
city, country  
E-Mail: email@address  
Phone: phonenumber

With best regards,

\_\_\_\_\_  
Signature\_1  
Title

\_\_\_\_\_  
Signature\_2  
title

This attestation is based on the template version 2.9 as of 2022-04-04, that was approved for use by ACAB-c.

CAB Footpage

page 1 of 8 pages

<p>Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor:</p>	<ul style="list-style-type: none"> <li>• CAB_company_name<sub>1</sub>, street, city, country registered under company_registration</li> <li>• Accredited by national_accreditation_body under registration accreditation_registration<sub>2</sub> for the certification of trust services according to "EN ISO/IEC 17065:2012" and "ETSI EN 319 403 V2.2.2 (2015-08)" and/or "ETSI EN 319 403-1 V2.3.1 (2020-06)" respectively.</li> <li>• Insurance Carrier (BRG section 8.2): &lt;&lt;&lt; name of insurance company &gt;&gt;&gt;</li> <li>• Third-party affiliate audit firms involved in the audit: none. &lt;&lt;&lt; ... or if any, provide names of audit firms and the jurisdictions in which they performed services &gt;&gt;&gt;</li> </ul>
<p>Identification and qualification of the audit team:</p>	<ul style="list-style-type: none"> <li>• Number of team members: &lt;&lt;&lt; state headcount &gt;&gt;&gt;</li> <li>• Academic qualifications of team members: All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security.</li> <li>• Additional competences of team members: All team members have knowledge of             <ol style="list-style-type: none"> <li>1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days;</li> <li>2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security;</li> <li>3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and</li> <li>4) the Conformity Assessment Body's processes.</li> </ol>             Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic.         </li> <li>• Professional training of team members:</li> </ul>

**Kommentiert [A4]:** State name and address of the organization performing the audit (<https://www.ccadb.org/policy#51-audit-statement-content>)

**Kommentiert [A5]:** Adapt, matching to your accreditation

**Kommentiert [A6]:** The Audit Team qualification statement is fully supported by ETSI EN 319 401/401-1. By this normative requirements, the Audit Team employed by the CAB must have the qualification, competences, experience as stated in this section.

**Please fill sections marked in yellow.**

If additional qualifications, competences, experiences were employed throughout the audit, please feel free to describes them here.

<sup>1</sup> in the following termed shortly "CAB"

<sup>2</sup> URL to the accreditation certificate hosted by the national accreditation body

This attestation is based on the template version 2.9 as of 2022-04-04, that was approved for use by ACAB-c.

	<p>See "Additional competences of team members" above. Apart from that are all team members trained to demonstrate adequate competence in:</p> <ul style="list-style-type: none"> <li>a) knowledge of the CA/TSP standards and other relevant publicly available specifications;</li> <li>b) understanding functioning of trust services and information security including network security issues;</li> <li>c) understanding of risk assessment and risk management from the business perspective;</li> <li>d) technical knowledge of the activity to be audited;</li> <li>e) general knowledge of regulatory requirements relevant to TSPs; and</li> <li>f) knowledge of security policies and controls.</li> </ul> <ul style="list-style-type: none"> <li>• Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting.</li> <li>• Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor             <ul style="list-style-type: none"> <li>a) has acted as auditor in at least three complete TSP audits;</li> <li>b) has adequate knowledge and attributes to manage the audit process; and</li> <li>c) has the competence to communicate effectively, both orally and in writing.</li> </ul> </li> <li>• Special skills or qualifications employed throughout audit: none. &lt;&lt;&lt; ...delete or add info if necessary for this audit &gt;&gt;&gt;</li> <li>• Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB. &lt;&lt;&lt; delete or add info if necessary for this audit &gt;&gt;&gt;</li> <li>• Auditors code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.</li> </ul>
<p>Identification and qualification of the reviewer performing audit quality management:</p>	<ul style="list-style-type: none"> <li>• Number of Reviewers/Audit Quality Managers involved independent from the audit team: &lt;&lt;&lt; state headcount &gt;&gt;&gt;</li> <li>• The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.</li> </ul>

**Kommentiert [A7]:** The Reviewers/ Audit Quality Manager qualification statement is fully supported by ETSI EN 319 401/401-1. By these normative requirements, the Reviewer employed by the CAB must have the qualification, competences, experience as stated in this section.

Please fill sections marked in yellow.

This attestation is based on the template version 2.9 as of 2022-04-04, that was approved for use by ACAB-c.

Audit Attestation <<Name>> <<Number>>

Identification of the CA/ Trust Service Provider (TSP):	<<< company name, street, city, country, registered under company registration >>>
---	--

**Kommentiert [A8]:** Full name of the CA (company) that was audited (<https://www.ccadb.org/policy#51-audit-statement-content>)

Type of audit:	<input type="checkbox"/> Point in time audit <input type="checkbox"/> Period of time, after x month of CA operation <input type="checkbox"/> Period of time, full audit
----------------	---

**Kommentiert [A9]:** State, whether the audit is for a period of time or a point in time. (<https://www.ccadb.org/policy#51-audit-statement-content>)

Audit period covered for all policies:	yyyy-mm-dd to yyyy-mm-dd or none, as audit was pit audit
--	--

**Kommentiert [A10]:** Start date and end date of the period that was audited, for those that cover a period of time (this is not the period the auditor was on-site) - see date format specifications below and <https://www.ccadb.org/policy#51-audit-statement-content>:

Point in time date:	yyyy-mm-dd or none, as audit was pot audit
---------------------	--

<date><space><splitter><space><date>  
Where splitter must be one of the following:

Audit dates:	yyyy-mm-dd to yyyy-mm-dd (remote) yyyy-mm-dd to yyyy-mm-dd (on site)
--------------	---

to  
through  
until  
and  
~  
~

Audit location:	locations
-----------------	-----------

Only the following date format is accepted according to ETSI TS 119 403-2. This applies to all occurrences of dates throughout the attestation:  
- YYYY-MM-DD example: 2016-05-07

No extra text within the date, such as "7th" or "the".  
If used, month names must be in English.

Standards considered:	<p>European Standards:</p> <input type="checkbox"/> ETSI EN 319 411-2, V2.2.2 (2018-04) <input type="checkbox"/> ETSI EN 319 411-1, V1.2.2 (2018-04) <input type="checkbox"/> ETSI EN 319 401, V2.2.1 (2018-04) <p>CA Browser Forum Requirements:</p> <input type="checkbox"/> EV SSL Certificate Guidelines, version 1.7.1 <input type="checkbox"/> Baseline Requirements, version 1.6.7 <p>Browser Policy Requirements:</p> <input type="checkbox"/> add or delete <p>Other:</p> <input type="checkbox"/> add or delete <p>For the Trust Service Provider Conformity Assessment:</p> <input checked="" type="checkbox"/> ETSI EN 319 403 V2.2.2 (2015-08) <input checked="" type="checkbox"/> ETSI TS 119 403-2 V1.2.4 (2020-11)
-----------------------	--

**Kommentiert [A11]:** Point in time date - see date format specifications below and <https://www.ccadb.org/policy#51-audit-statement-content>:

Only the following date format is accepted according to ETSI TS 119 403-2. This applies to all occurrences of dates throughout the attestation:  
- YYYY-MM-DD example: 2016-05-07

No extra text within the date, such as "7th" or "the".  
If used, month names must be in English.

**Kommentiert [A12]:** Full names and version numbers of the audit standards that were used during the audit. (<https://www.ccadb.org/policy#51-audit-statement-content>)

This attestation is based on the template version 2.9 as of 2022-04-04, that was approved for use by ACAB-c.

Audit Attestation <<Name>> <<Number>>

The full annual audit was based on the following policy and practice statement documents of the CA / TSP:

1. document\_1, version x.y, as of yyyy-mm-dd
2. document\_2, version x.y, as of yyyy-mm-dd
3. ...

**Kommentiert [A13]:** A statement to indicate that (!) the audit was a full audit. **Note:** Surveillance audits are not acceptable following the Browser Root Store Policies! (<https://www.ccadb.org/policy#51-audit-statement-content>)

**Kommentiert [A14]:** List of the CA policy documents (with version numbers) referenced during the audit. (<https://www.ccadb.org/policy#51-audit-statement-content>)

No major or minor non-conformities have been identified during the audit. ///

In the following areas, non-conformities have been identified throughout the audit:

**Kommentiert [A15]:** Choose the applicable paragraph and list the non-conformities. All identified non-conformities have to be listed, not only the open one's!

Findings with regard to ETSI EN 319 401:

7.2 Human resources

Documentation and implementation of ...xyz... shall be improved. [REQ-7.2-xx, REQ-7.2-yy]

7.4 Access control

Documentation and implementation of ...xyz... shall be improved. [REQ-7.4-xy]

7.8 Network security

Documentation and implementation of ...xyz... shall be improved. [REQ-7.8-xy]

Findings with regard to ETSI EN 319 411-1:

None.

Findings with regard to ETSI EN 319 411-2:

None.

All non-conformities have been closed before the issuance of this attestation. ///

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit. ///

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

**Kommentiert [A16]:** Choose the applicable paragraph.

This Audit Attestation also covers the following incidents as documented under

- Bug xyz, TSP Name: Incident description:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=...](https://bugzilla.mozilla.org/show_bug.cgi?id=...)
- ...
- Bug xyz, TSP Name: Incident description:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=...](https://bugzilla.mozilla.org/show_bug.cgi?id=...)
- ...

**Kommentiert [A17]:** Must match with Bugzilla incident listing of last day of the audit period covered with this AAL.

This attestation is based on the template version 2.9 as of 2021-xx-xx, that was approved for use by ACAB-c.

The remediation measures taken by [TSP Name] as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

This attestation is based on the template version 2.9 as of 2022-04-04, that was approved for use by ACAB-c.

CAB Footpage

page 6 of 8 pages

Audit Attestation <<Name>> <<Number>>

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
Complete subject DN: Example: CN = ABC Root CA, O = ABC Co., C = DE	SHA-256 fingerprint of the certificate:  Example: FC8BBF7D278D2E5F070BCEF6FAF3AAB1BEF30DA3EB2875424295AD147F2AAF07	ETSI EN policy that this Root has been assessed against:  Example: ETSI EN 319 411-2 V2.2.2, QCP-w

Table 1: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
Complete subject DN: Example: CN = ABC Issuing CA, O = ABC Co., C = DE	SHA-256 fingerprint of the certificate:  Example: BC8BBF7D278D2E5F070BCEF6FAF3AAB1BEF30DA3EB2875424295AD147F2AAF08	ETSI EN policy that this Root has been assessed against:  Example: ETSI EN 319 411-2 V2.2.2, QCP-w	EKU of the CA or: state "not defined"  Example: 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)

Table 2: Sub-CA's issued by the Root-CA or its Sub-CA's in scope of the audit

This attestation is based on the template version 2.9 as of 2021-04-04, that was approved for use by ACAB-c.

**Kommentiert [A18]:** Requirements for SHA-256 fingerprint:  
 - MUST: No colons, no spaces, and no line feeds  
 - MUST: Uppercase letters  
 - MUST: be encoded in the document (PDF) as text searchable, not an image  
**Must be the hash value of DER representation!**  
<https://www.ccadb.org/policy#51-audit-statement-content>

**Kommentiert [A19]:** Make sure there is no linefeed or page brake to allow automated reading of the values given!

**Kommentiert [A20]:** Full names and version numbers of the audit standards that were used during the audit; and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers).  
<https://www.ccadb.org/policy#51-audit-statement-content>

**Kommentiert [A21]:** Requirements for SHA-256 fingerprint:  
 - MUST: No colons, no spaces, and no line feeds  
 - MUST: Uppercase letters  
 - MUST: be encoded in the document (PDF) as text searchable, not an image

**Must be the hash value of DER representation!**  
**Kommentiert [A22]:** Make sure there is no linefeed or page brake to allow automated reading of the values given!

**Kommentiert [A23]:** Full names and version numbers of the audit standards that were used during the audit; and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers).  
<https://www.ccadb.org/policy#51-audit-statement-content>

Audit Attestation <<Name>> <<Number>>

**Modifications record**

Version	Issuing Date	Changes
Version 1	yyyy-mm-dd	Initial attestation
Version 1.1	yyyy-mm-dd	1st amended attestation
...	...	...

**End of the audit attestation letter.**

This attestation is based on the template version 2.9 as of 2021-04-04, that was approved for use by ACAB-c.