

INDEPENDENT ASSURANCE REPORT

To the management of the Government Authority for Electronic Certification of the People's Democratic Republic of Algeria ("Autorité Gouvernementale de Certification Electronique" or "AGCE"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on AGCE management's statement that for its Certification Authority (CA) operations in Algiers, Algeria and Annaba, Algeria throughout the period 1 April 2021 to 31 March 2022 (the "Period") for its:

1. Government CA
2. Infrastructure CA
3. Corporate CA

AGCE has:

- disclosed its SSL certificate lifecycle management business practices in its:
 - [Government Certification Authority CP/CPS, v1.1, 25 October 2020](#);
 - [Government Certification Authority CP/CPS, v1.2, 01 October 2021](#);
 - [AGCE Infrastructure Certification Authority CPS, v1.4, 25 October 2020](#);
 - [AGCE Infrastructure Certification Authority CP/CPS, v1.5, 01 October 2021](#);
 - [AGCE Corporate Certification Authority CPS, v1.3, 25 October 2020](#) and
 - [AGCE Corporate Certification Authority CPS, v1.4, 01 October 2021](#)
- including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the AGCE website which is available at <https://ca.pki.agce.dz/repository>, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
 - SSL subscriber information is properly authenticated (for the registration activities performed by AGCE)
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.5](#).

Certification authority's responsibilities

AGCE's management is responsible for its statement, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.5.

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.



The firm applies Canadian Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's statement based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's statement is fairly stated, and, accordingly, included:

- (1) obtaining an understanding of AGCE's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of AGCE's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- (2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;
- (3) testing and evaluating the operating effectiveness of the controls; and
- (4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at AGCE and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, AGCE's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Basis for qualified opinion

During our procedures, we noted the following which caused a qualification of our opinion:

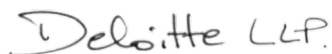
Observation	Relevant WebTrust Criteria
<p>1 During the Period, we noted an instance where lapsed time between Certificate Systems Vulnerability Scans has exceeded three months</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5, Principle 4, Criterion 4.3 to not be met.</p>	<p>P4, 4.3: The CA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following:</p> <ul style="list-style-type: none">• Within one (1) week of receiving a request from the CA/Browser Forum;• After any system or network changes that the CA determines are significant;• and• At least every three (3) months
<p>2 During the Period, there were instances where time from the discovery of a Critical Vulnerability to remediation of the vulnerability or creation and implementation of a plan to mitigate the vulnerability or</p>	<p>P4, 4.6: The CA maintains controls to provide reasonable assurance that it performs one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process:</p> <ul style="list-style-type: none">• Remediate the Critical Vulnerability;

Observation	Relevant WebTrust Criteria
<p>documentation of the factual basis for determination that the vulnerability does not require remediation exceeded 96 hrs.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5, Principle 4, Criterion 4.6 to not be met.</p>	<ul style="list-style-type: none"> • If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: <ul style="list-style-type: none"> ○ Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and ○ Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; OR • Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: <ul style="list-style-type: none"> ○ The CA disagrees with the NVD rating; ○ The identification is a false positive; ○ The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or ○ Other similar reasons.

Practitioner's qualified opinion

In our opinion, except for the matters described in preceding paragraph, throughout the period 1 April 2021 to 31 March 2022, AGCE management's statement, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.5.

This report does not include any representation as to the quality of AGCE's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.5, nor the suitability of any of AGCE's services for any customer's intended purpose.



Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
8 July 2022



CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
1	1	C = DZ, O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE, CN = Government CA	C=DZ, O=AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE, CN=National Root CA	76d69ae5965319c32cc028a00854bca3d06aada	RSA 4096-bit	SHA 256	Mar 10 13:35:02 2020 GMT	Mar 10 13:35:02 2037 GMT		2DAEEA9E153FCAE2FC169E79FADF841E14EFE5EA	4283BBC4124666640C945C608BC59F5EB6B4DE0BD70E3D34A78EC7CA2720B138
2	1	C = DZ, O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE, CN = Infrastructure CA	C = DZ, O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE, CN = Government CA	45ee75ecd9316864f14e10abf11b5f60ef874cde	RSA 4096-bit	SHA 256	Mar 17 00:48:49 2020 GMT	Mar 17 00:48:49 2028 GMT		06EAC0891B1C2F3621217C8299AD61D42D367763	84799F0649C37341D24BF08B5D68A1144A134FAED0D88CEE5A8C1C2788ED8E40
3	1	C = DZ, O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE, CN = Corporate CA	C = DZ, O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE, CN = Government CA	0462cff38515f732b685c6f90b67912d0cf02480	RSA 4096-bit	SHA 256	Mar 17 00:42:40 2020 GMT	Mar 17 00:42:40 2028 GMT		0EE5E13DEB47C003DBD5BC55A9CCD5CBFC181F34	6B872DFD67DE32C65F94B2A68CB35A8A10697C52262D771BD067C60CB2A9FCF1



PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
GOVERNMENT ELECTRONIC CERTIFICATION AUTHORITY

General Manager

Réf.....134...../GM/AGCE/2022



GOVERNMENT AUTHORITY FOR ELECTRONIC CERTIFICATION
AGCE MANAGEMENT'S STATEMENT

Government Authority for Electronic Certification of the People's Democratic Republic of Algeria ("Autorité Gouvernementale de Certification Electronique" or "AGCE") operates the Certification Authority (CA) services known as:

1. Government CA
2. Infrastructure CA
3. Corporate CA

The management of AGCE is responsible for establishing controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL certificate lifecycle management controls on its website which is available at <https://ca.pki.agce.dz/repository>. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to AGCE's operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

AGCE management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in AGCE management's opinion, in providing its Certification Authority (CA) services in Algiers, Algeria and Annaba, Algeria, throughout the period 16 November 2020 to 31 March 2021, AGCE has:

- disclosed its SSL certificate lifecycle management business practices in in its:
 - [Government Certification Authority CP/CPS, v1.1, 25 October 2020;](#)
 - [Government Certification Authority CP/CPS, v1.2, 01 October 2021;](#)
 - [AGCE Infrastructure Certification Authority CPS, v1.4, 25 October 2020;](#)
 - [AGCE Infrastructure Certification Authority CP/CPS, v1.5, 01 October 2021;](#)
 - [AGCE Corporate Certification Authority CPS, v1.3, 25 October 2020;](#) and
 - [AGCE Corporate Certification Authority CPS, v1.4, 01 October 2021.](#)

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the AGCE website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
 - SSL subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.5](#).

Mrs ZAHIA BRAHIMI

AGCE DIRECTOR (AGCE General Manager)

Autorité Gouvernementale de Certification Electronique

8 July 2022

Directrice Générale de l'Autorité
Gouvernementale de Certification
Electronique
Signature: Zahia BRAHIMI

