

## 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 business, key lifecycle management, certificate lifecycle management, and CA environmental control 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](#); and
  - [AGCE Infrastructure Certification Authority CP/CPS, v1.5, 01 October 2021](#);
  - [AGCE Corporate Certification Authority CPS, v1.3, 25 October 2020](#)
  - [AGCE Corporate Certification Authority CPS, v1.4, 01 October 2021](#);
- maintained effective controls to provide reasonable assurance that:
  - AGCE's Certification Practice Statements are consistent with its Certificate Policy; and
  - AGCE provides its services in accordance with its Certificate Policy and Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by AGCE); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

AGCE does not escrow its CA keys, does not provide subscriber key generation, storage and recovery services, does not provide integrated circuit card management services, and does not provide third-party subordinate CA or cross certificate issuance or management. Accordingly, our procedures did not extend to controls that would address those criteria.

### 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 v2.2.2](#).



### **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 key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
- (2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business 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**

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.



#### **Practitioner's opinion**

In our opinion, 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 v2.2.2](#).

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 v2.2.2](#), nor the suitability of any of AGCE's services for any customer's intended purpose.

#### **Use of the WebTrust seal**

AGCE's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

A handwritten signature in black ink that reads "Deloitte LLP".

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	76d69ae5965319c32cc028a00854bca3d06aadaf	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



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")

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

The management of AGCE is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website which is available at <https://ca.pki.agce.dz/repository>, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. 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 1 April 2021 to 31 March 2022, AGCE has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control 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](#)





maintained effective controls to provide reasonable assurance that:

AGCE's Certification Practice Statements are consistent with its Certificate Policy; and

AGCE provides its services in accordance with its Certificate Policy and Certification Practice Statements

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by AGCE); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems' integrity

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), including the following:

#### **CA Business Practices Disclosure**

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

#### **CA Business Practices Management**

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

#### **CA Environmental Controls**

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

## CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

## Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

## Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

AGCE does not escrow its CA keys, does not provide subscriber key generation, storage and recovery services, does not provide integrated circuit card management services, and does not provide third-party subordinate CA or cross certificate issuance or management.

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

