Deloitte LLP
Bay Adelaide Centre, East Tower
8 Adelaide Street West
Suite 200
Toronto, ON M5H 0A9
Canada

Tel: +1 416 601 6150
Fax: +1 416 601 6400
www.deloitte.ca

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 Électronique" 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 1st October 2022 to 30 September 2023 (the "Period") for its CAs as enumerated in Attachment A1, AGCE has:

- disclosed its SSL certificate lifecycle management business practices in its:
    - Government Certification Authority CP/CPS v2.2, 14 September 2023
    - Government Certification Authority CP/CPS v2.1, 22 June 2023
    - Government Certification Authority CP/CPS v2.0, 25 June 2022
    - AGCE CPS for Legal and Natural Person v2.2, 14 September 2023
    - AGCE CPS for Legal and Natural Person v2.1, 22 June 2023
    - AGCE CPS for Legal and Natural Person v2.0, 25 June 2022
    - AGCE CPS for Devices v2.2, 14 September 2023
    - AGCE CPS for Devices v2.1, 22 June 2023
    - AGCE CPS for Devices v2.0, 25 June 2022

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the AGCE website and provide 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 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;

And for its CAs as enumerated in Attachment A2:

- 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 v2.6.

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 v2.6.

Our independence and quality management

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behaviour.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services 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 International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. 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 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

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 1st October 2022 to 30 September 2023, 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 v2.6.

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 v2.6, 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 – SSL Baseline with Network Security 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.

Deloitte LLP.

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
26 December 2023

ATTACHMENT A1

LIST OF IN-SCOPE CAs FOR SSL BASELINE REQUIREMENTS

Intermediate CAs
2. Government TLS CA 4. Government SMIME CA 6. Government CA
Issuing CAs that issued Subscriber Certificates during the Period
8. OV TLS CA 9. SMIME CA
Issuing CAs that have not issued any Subscriber Certificates during the Period
12. Corporate CA 13. Infrastructure CA

ATTACHMENT A2

LIST OF IN-SCOPE CAs FOR NETWORK SECURITY REQUIREMENTS

Intermediate CAs

1. Government CA 2022
2. Government TLS CA
3. Government CS CA
4. Government SMIME CA
5. Government TS CA
6. Government CA

Issuing CAs that issued Subscriber Certificates during the Period

7. Corporate CA 2022
8. OV TLS CA
9. SMIME CA

Issuing CAs that have not issued any Subscriber Certificates during the Period

10. Code Signing CA
11. Trust Services CA
12. Corporate CA
13. Infrastructure CA

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Extended Key Usage	EKU [RFC5280]	Subject Key Identifier	SHA256 Fingerprint
1	1	CN = Government CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = National Root CA O = AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE C = DZ	324DB2A42674602348782F66428B991F25C955B9	RSA 4096-bit	SHA 256	13 June 2022 15:30:18	13 June 2039 15:30:18	TLS Web Client Authentication	id-kp-clientAuth	C9EDA480BB519F1310692D90E1B775935E25B872	9D75BA327B190DC593CE3F666BFD2E5C9B38CB530F94875A7DF7524112589A73
2	1	CN = Government TLS CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = National Root CA O = AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE C = DZ	11B5CF75CB580111D73FDF2B363E53A17A571AAB	RSA 4096-bit	SHA 256	13 June 2022 15:51:33	13 June 2039 15:51:33	TLS Web Client Authentication, TLS Web Server Authentication	id-kp-clientAuth, id-kp-serverAuth	09AEF0917F30A3FEBB6845F111E559A95C5D893A	F0FA7AF4E8FD1E397C9CC534EB0DE4D6B065D63D62C53BE55572465284AA1240
3	1	CN = Government CS CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = National Root CA O = AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE C = DZ	564398E06302C669B27C0DEE4A452360FB1F04E2	RSA 4096-bit	SHA 256	13 June 2022 16:13:01	13 June 2039 16:13:01	Code Signing	id-kp-codeSigning	C6A1145DA124292386770DEB0C76EB9EFDE649C1	82DA1AC4781ECC6013C7F925D98C8C36636909D87EDC94ECB0DE9518B742E45E
4	1	CN = Government SMIME CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = National Root CA O = AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE C = DZ	57543FFDB47FE5722070E30485F6F2D488DF036A	RSA 4096-bit	SHA 256	13 June 2022 16:04:07	13 June 2039 16:04:07	E-mail Protection	id-kp-emailProtection	D52E64EE3B119342B6D05BB1ABDD8DC90ABDA111	3F7E684A13653F9B941AEE054DF23A5236F495AAC0916CFA1E22F14ED6655E7E
5	1	CN = Government TS CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = National Root CA O = AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE C = DZ	0ED20535D3DC3577753FAA33CC3551D162CF2159	RSA 4096-bit	SHA 256	13 June 2022 16:20:41	13 June 2039 16:20:41	Time Stamping	id-kp-timeStamping	CF73D19C9965CE555EB80D9A9D154A3C8ABF1FC7	DAEE98D82A3F92A494893D9CF3163469ECA6EFA7A50D98810661D436413528E3
6	1	CN = Government CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = National Root CA O = AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE C = DZ	76D69AE5965319C32CC028A00854BCA3D06AADAF	RSA 4096-bit	SHA 256	10 March 2020 14:35:02	10 March 2037 14:35:02			2DAEEA9E153FCAE2FC169E79FADF841E14EFE5EA	4283BBC4124666640C945C608BC59F5EB6B4DE0BD70E3D34A78EC7CA2720B138
7	1	CN = Corporate CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = Government CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	0189E93D39414F3E3D6D08E4EC2C35CA34B4A85F	RSA 4096-bit	SHA 256	14 June 2022 13:51:18	14 June 2031 13:51:18	TLS Web Client Authentication	id-kp-clientAuth	EBAEA64C2164FDDB6E70B94A36689B10A1D20772	871B0E1C3A8ED6333A82FF1317B086465D5CFB332121F1479A05251709C7BAD7
8	1	CN = OV TLS CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = Government TLS CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	13FFE98E37FDBF07F4498FAD8737EFFD6E5FF6E9	RSA 4096-bit	SHA 256	14 June 2022 14:08:41	14 June 2031 14:08:41	TLS Web Client Authentication, TLS Web Server Authentication	id-kp-clientAuth, id-kp-serverAuth	8F51DEFBD29136BC27E3454F96A7CA25B2E75E49	7FAE1EF2FE0FC89E24535A7DD19F0C18E3D76CD873E417F4920DCBBBBB958050
9	1	CN = SMIME CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = Government SMIME CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	072A9B7F19238578FEC699601A7E64F665D016B4	RSA 4096-bit	SHA 256	14 June 2022 14:11:19	14 June 2031 14:11:19	E-mail Protection	id-kp-emailProtection	A3AB9CA6C0A410DC71AC17A693EF0FC267412293	6D7B5AAA08F169C25468D8CF3AAD579C2BEA1BEB89CC220123ED374437C548F4
10	1	CN = Code Signing CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = Government CS CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	483EAE7224857CF133C78CECB85FD23D19435D1D	RSA 4096-bit	SHA 256	14 June 2022 14:23:15	14 June 2031 14:23:15	Code Signing	id-kp-codeSigning	45728DAA4639A04F3730C8AB5658DCD868AF0843	99F69BAE1AA63D560A2603CA300BD9FA883AC61C1F7932461678C5EF698421BA
11	1	CN = Trust Services CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = Government TS CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	2EB8EFE3A0E0A1161D3C1F9FDF2081E2FE89836B	RSA 4096-bit	SHA 256	14 June 2022 14:26:24	14 June 2031 14:26:24	Time Stamping	id-kp-timeStamping	F535E2AEF08EADDD8CCAAF216573D24D9C33EDF7	36BD6CD486D0164C44C846B37A4448E1AE124843F2B432CF9D4BC1D86AB2D0D9
12	1	CN = Corporate CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = Government CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	0462CFF38515F732B685C6F90B67912D0CF02480	RSA 4096-bit	SHA 256	17 March 2020 01:42:40	17 March 2028 01:42:40			0EE5E13DEB47C003DBD5BC55A9CCD5CBFC181F34	6B872DFD67DE32C65F94B2A68CB35A8A10697C52262D771BD067C60CB2A9FCF1
13	1	CN = Infrastructure CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	CN = Government CA O = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE C = DZ	45EE75ECD9316864F14E10ABF11B5F60EF874CDE	RSA 4096-bit	SHA 256	17 March 2020 01:48:49	17 March 2028 01:48:49			06EAC0891B1C2F3621217C8299AD61D42D367763	84799F0649C37341D24BF08B5D68A1144A134FAED0D88CEE5A8C1C2788ED8E40

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

GOVERNMENT ELECTRONIC CERTIFICATION AUTHORITY

General Manager

Réf :228/GM/AGCE/2023

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 Électronique" or "AGCE") operates the Certification Authority (CA) services as enumerated in Attachment A1 and provides SSL CA services.

Government Authority for Electronic Certification of the People's Democratic Republic of Algeria ("Autorité Gouvernementale de Certification Électronique" or "AGCE") operates the Certification Authority (CA) services as enumerated in Attachment A2 and provides non-SSL CA services.

The management of AGCE is responsible for establishing and maintaining effective 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 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.

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 at Algiers, Algeria, and Annaba, Algeria, throughout the period 1st October 2022 to 30 September 2023, AGCE has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Government Certification Authority CP/CPS v2.2, 14 September 2023
  - Government Certification Authority CP/CPS v2.1, 22 June 2023
  - Government Certification Authority CP/CPS v2.0, 25 June 2022
  - AGCE CPS for Legal and Natural Person v2.2, 14 September 2023
  - AGCE CPS for Legal and Natural Person v2.1, 22 June 2023
  - AGCE CPS for Legal and Natural Person v2.0, 25 June 2022
  - AGCE CPS for Devices v2.2, 14 September 2023

    - AGCE CPS for Devices v2.1, 22 June 2023
    - AGCE CPS for Devices v2.0, 25 June 2022

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the AGCE website and provide 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 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;

- 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 v2.6.

Mrs ZAHIA BRAHIMI
AGCE DIRECTOR (AGCE General Manager)
Autorité Gouvernementale de Certification Électronique
26 December 2023

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

السلطة الحكومية للتصديق الإلكتروني
الجمهورية الجزائرية الديمقراطية الشعبية
المدير العام

ATTACHMENT A1

LIST OF IN-SCOPE CAs FOR SSL BASELINE REQUIREMENTS

Intermediate CAs
2. Government TLS CA 4. Government SMIME CA 6. Government CA
Issuing CAs that issued Subscriber Certificates during the Period
8. OV TLS CA 9. SMIME CA
Issuing CAs that have not issued any Subscriber Certificates during the Period
12. Corporate CA 13. Infrastructure CA

ATTACHMENT A2

LIST OF IN-SCOPE CAs FOR NETWORK SECURITY REQUIREMENTS

Intermediate CAs
1. Government CA 2022 2. Government TLS CA 3. Government CS CA 4. Government SMIME CA 5. Government TS CA 6. Government CA
Issuing CAs that issued Subscriber Certificates during the Period
7. Corporate CA 2022 8. OV TLS CA 9. SMIME CA
Issuing CAs that have not issued any Subscriber Certificates during the Period
10. Code Signing CA 11. Trust Services CA 12. Corporate CA 13. Infrastructure CA