

## REPORT OF THE INDEPENDENT ACCOUNTANT

*To the management of SSLCOM GROUP Ltd. ("SSLCOM GROUP"):*

### Scope

We have been engaged, in a reasonable assurance engagement, to report on SSLCOM GROUP management's assertion that for its Certification Authority (CA) operations at HaBarzel St. 27, Tel Aviv-Yafo, ISRAEL, throughout the period from March 11, 2019 through February 24, 2020, for its self-signed Root and Subordinate CAs as enumerated in "Attachment A" SSLCOM GROUP has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - [SSLCOM GROUP's Certification Practice Statement \(CPS\) Version 1.3](#) including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the SSLCOM GROUP website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, 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 SSLCOM GROUP)
- suitably designed, and placed into operation, 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
- suitably designed, and placed into operation, 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
- suitably designed, and placed into operation, 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 v2.4.1](#).



### **Certification authority's responsibilities**

SSLCOM GROUP's management is responsible for its assertion, 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 v2.4.1.](#)

### **Our independence and quality control**

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 Control 1, 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.

### **Auditor's responsibilities**

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, Assurance Engagements. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- (1) obtaining an understanding of SSLCOM GROUP's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, and revocation of SSL certificates, obtaining an understanding of SSLCOM GROUP's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- (2) evaluating the suitability of the design of the controls; and
- (3) performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of SSLCOM GROUP's controls, individually or in the aggregate.

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

### **Suitability of controls**

The suitability of the design of the controls at SSLCOM GROUP 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 suitability of the design of the controls at individual subscriber and relying party locations.

<b>Tel Aviv</b>	<b>Jerusalem</b>	<b>Haifa</b>	<b>Beer Sheva</b>	<b>Bene Berak</b>	<b>Kiryat Shmona</b>	<b>Petach Tikva</b>	<b>Modiin Ilit</b>	<b>Nazareth</b>	<b>Eilat</b>
+972-3-6386868	+972-2-6546200	+972-4-8680600	+972-77-7784100	+972-73-7145300	+972-77-5054906	+972-77-7784180	+972-8-9744111	+972-4-6555888	+972-8-6339911

**Head Office:** Amot BDO House, 48 Menachem Begin Road, Tel Aviv 6618001, ISRAEL **Email:** [bdo@bdo.co.il](mailto:bdo@bdo.co.il) **Our Site:** [www.bdo.co.il](http://www.bdo.co.il)

BDO Israel, an Israeli partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms



### Inherent limitations

Because of the nature and inherent limitations of controls, SSLCOM GROUP'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.

### Opinion

In our opinion, throughout the period from March 11, 2019 through February 24, 2020,, SSLCOM GROUP management's assertion, 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 v2.4.1](#).

This report does not include any representation as to the quality of SSLCOM GROUP's services beyond those covered by [the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1](#), nor the suitability of any of SSLCOM GROUP's services for any customer's intended purpose.

Ziv Haft

Certified Public Accountants (Isr.)  
BDO Member Firm

Tel-Aviv, Israel  
February 25, 2020

Tel Aviv	Jerusalem	Haifa	Beer Sheva	Bene Berak	Kiryat Shmona	Petach Tikva	Modiin Ilit	Nazareth	Eilat
+972-3-6386868	+972-2-6546200	+972-4-8680600	+972-77-7784100	+972-73-7145300	+972-77-5054906	+972-77-7784180	+972-8-9744111	+972-4-6555888	+972-8-6339911

Head Office: Amot BDO House, 48 Menachem Begin Road, Tel Aviv 6618001, ISRAEL Email: [bdo@bdo.co.il](mailto:bdo@bdo.co.il) Our Site: [www.bdo.co.il](http://www.bdo.co.il)

BDO Israel, an Israeli partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms

## Attachment A

	<b>Almost Free SSL RootCA G1</b>	<b>SSLCom Root G1</b>
Signature hash algorithm	SHA256	SHA256
Subject	CN = Almost Free SSL RootCA G1 OU = Certificate Services O = SSLCom Group Ltd. C = IL	CN = SSLCom Root G1 OU = Certificate Services O = SSLCom Group Ltd. C = IL
Thumbprint	a9 3f e6 32 09 e8 65 72 7c 81 04 5f da 5a 64 e3 b6 3e 1b 92	c8 33 d0 8a 9f 6c 5c 28 b4 60 0d 7e 8f 33 70 4d 4f e5 07 3a

	<b>Pythagoras Secure TLS CA G1</b>	<b>Fermat Crypto TLS CA G1</b>	<b>Almost Free SSL CA G1</b>
Signature hash algorithm	SHA256	SHA256	SHA256
Subject	CN = Pythagoras Secure TLS CA G1 OU = Certificate Services O = SSLCom Group Ltd. C = IL	CN = Fermat Crypto TLS CA G1 OU = Certificate Services O = SSLCom Group Ltd. C = IL	CN = Almost Free SSL CA G1 OU = Certificate Services O = SSLCom Group Ltd. C = IL
Thumbprint	51 47 5e 89 d4 32 b3 c2 5f 7a 7c f7 16 62 9b bd bb 34 9c 12	4e 2e 6f 0a a1 4d e8 30 7a cd 81 5c 44 26 de 70 83 63 c8 1a	72 56 0b 44 38 f1 b5 13 17 21 c9 a9 bc e6 83 86 1a 3f 22 bc

	<b>SSLCom TLS DV CA G1</b>	<b>Almost Free SSL DV CA G1</b>	<b>SSLCom Secure Certification Authority G1</b>
Signature hash algorithm	SHA256	SHA256	SHA256
Subject	CN = SSLCom TLS DV CA G1 OU = Certificate Services O = SSLCom Group Ltd. C = IL	CN = Almost Free SSL DV CA G1 OU = Certificate Services O = SSLCom Group Ltd. C = IL	CN = SSLCom Secure Certification Authority G1 OU = Certificate Services O = SSLCom Group Ltd. C = IL
Thumbprint	bd 29 2e 74 14 f5 67 d4 0d d2 e5 74 c8 fb c4 c7 3f 83 7f 5c	5c 99 ac d6 3d f7 f2 09 25 94 1a b8 c6 7c ac b4 5a 46 a7 f7	bb e8 83 36 82 e4 6f 6f d9 74 76 7c 20 c2 76 ad 40 fa 20 23

	<b>SSLCom Secure TLS DV CA G1</b>	<b>Almost Free SSL DV CA G1</b>
Signature hash algorithm	SHA256	SHA256
Subject	CN = SSLCom Secure TLS DV CA G1 OU = Certificate Services O = SSLCom Group Ltd. C = IL	CN = Almost Free SSL Secure DV CA G1 OU = Certificate Services O = SSLCom Group Ltd. C = IL
Thumbprint	c1 23 e9 af 6b 81 78 ba 02 22 b8 7f dd a1 1c 1f fc e4 08 36	6c 2e b6 56 d6 72 e3 18 5c 4a 9d 5c 19 4b 70 30 f0 13 e9 54

Tel Aviv | Jerusalem | Haifa | Beer Sheva | Bene Berak | Kiryat Shmona | Petach Tikva | Modiin Ilit | Nazareth | Eilat  
 +972-3-6386868 | +972-2-6546200 | +972-4-8680600 | +972-77-7784100 | +972-73-7145300 | +972-77-5054906 | +972-77-7784180 | +972-8-9744111 | +972-4-6555888 | +972-8-6339911

**Head Office:** Amot BDO House, 48 Menachem Begin Road, Tel Aviv 6161001, ISRAEL **Email:** bdo@bdo.co.il **Our Site:** www.bdo.co.il

BDO Israel, an Israeli partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms

## SSLCOM GROUP LTD MANAGEMENT'S ASSERTION

**SSLCOM GROUP LTD.** ("SSLCOM GROUP") operates the Certification Authority (CA) services known as, Root: Almost Free SSL RootCA G1, SSLCom Root G1 and Subordinate CAs: Pythagoras Secure TLS CA G1, Fermat Crypto TLS CA G1, Almost Free SSL CA G1, SSLCom TLS DV CA G1, Almost Free SSL DV CA G1, SSLCom Secure Certification Authority G1, SSLCom Secure TLS DV CA G1, Almost Free SSL DV CA G1 and provides SSL CA services.

SSLCOM GROUP management has assessed its controls over its SSL Certification Authority (CA) services at HaBarzel St. 27, Tel Aviv-Yafo, ISRAEL, throughout the period from March 11, 2019 through February 24, 2020, SSLCOM GROUP has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - [SSLCom CPS v1.3](#)including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the SSLCOM GROUP website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, 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 SSLCOM GROUP)
- suitably designed, and placed into operation, 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
- suitably designed, and placed into operation, 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 v2.4.1.](#)

Yosi Rosner, CEO

SSLCOM GROUP LTD.

