SHARONY – SHEFLER & CO. C.P.A. **שרוני - שפלר ושות'** רואי חשבון

SHARONY ARIE	C.P.A. (ISR.)	רואה חשבון	**שרוני אריה**
SHEFLER ELI	C.P.A. (ISR.)	רואה חשבון	**שפלר אלי**
SHEFLER EREZ	C.P.A. (ISR.)	רואה חשבון	**שפלר ארז**
ESHEL BARUCH	C.P.A. (ISR.)	רואה חשבון	**אשל ברוך**
DARVISH TZION	C.P.A. (ISR.)	רואה חשבון	**דרויש ציון**
PRIESS HANA	C.P.A. (ISR.)	רואה חשבון	**פרייס חנה**
BERMAN GIL	C.P.A. (ISR.), Adv.	רואה חשבון, עורך דין	**ברמן גיל**
LEIBOVITCH SHLOMO	C.P.A. (ISR.)	רואה חשבון	**לייבוביץ שלמה**
SHAYZAF JACOB	Eng., M.Sc	מהנדס, תעשיה וניהול	**שיזף יעקב**

March 10, 2019

REPORT OF THE INDEPENDENT ACCOUNTANT

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

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, as of March 10, 2019, for its self-signed Root Keys CAs as enumerated in "Attachment A" SSLCOM GROUP has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
  - SSLCOM GROUP's Certification Practice Statement (CPS) Version 1.0
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - SSLCOM GROUP provides its services in accordance with its Certification Practice Statement.
- suitably designed, and placed into operation, 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 SSLCOM GROUP; and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.1.

SSLCOM GROUP does not escrow its CA keys, does not provide subscriber key generation services, does not provide subscriber key management services, does not provide OCSP services and does not provide subscriber key storage and recovery services and does not provide certificate suspension services. Accordingly, our audit did not extend to controls that would address those criteria.

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 v2.1.

The relative effectiveness and significance of specific 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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

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 attestation standards established by the American Institute of Certified Public Accountants. 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 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) 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.

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, as of February 28, 2019 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 v2.1

This report does not include any representation as to the quality of SSLCOM GROUP's services than its CA operations at HaBarzel St. 27, Tel Aviv-Yafo, ISRAEL, nor the suitability of any of SSLCOM GROUP's services for any customer's intended purpose.

Erez Shefler, CPA, CISA, CRISC, CIA, CRMA
Sharony - Shefler & Co.
Certified Public Accountants (Isr.)

March 10, 2019

Attachment A

	Almost Free SSL RootCA G1
Signature hash algorithm	SHA256
Subject	CN = Almost Free SSL RootCA 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

	Pythagoras Secure TLS CA G1	**Fermat Crypto TLS CA G1**	**Almost Free SSL CA G1**
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

SSLCOM GROUP LTD MANAGEMENT'S ASSERTION

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

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation - this service is under construction
- Subscriber key generation and management
- Subordinate CA certification

The management of SSLCOM GROUP LTD is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, 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 SSLCOM GROUP LTD's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

SSLCOM GROUP LTD management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in SSLCOM GROUP LTD management's opinion, in providing its Certification Authority (CA) services at HaBarzel St. 27, Tel Aviv-Yafo, ISRAEL, as of March 10, 2019, SSLCOM GROUP LTD has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
    - SSLCom CPS v1.0

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - SSLCOM GROUP LTD's Certification Practice Statement is consistent with its Certificate Policies
    - SSLCOM GROUP LTD provides its services in accordance with its Certification Practice Statement

- suitably designed, and placed into operation, 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 SSLCOM GROUP LTD); and
    - subordinate CA certificate requests are accurate, authenticated, and approved

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.1, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

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

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- 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 and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation - this service is under construction

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

Yosi Rosner, CEO

SSLCOM GROUP LTD.