



StartCom CA Limited

Independent's Practitioner Reasonable Assurance Report



INDEPENDENT'S PRACTITIONER REASONABLE ASSURANCE REPORT

To the management of StartCom CA Limited:

We have undertaken a reasonable assurance engagement on the accompanying statement by the management of the Certification Authority of StartCom (onwards, "CA-StartCom") that in providing its Certification Authority services through the "StartCom Root" (StartCom Certification Authority G3 with hash algorithm SHA256 and fingerprint 68 9a 12 29 d6 98 d1 72 e9 9e 1b f0 ob 9c 19 85 41 19 c9 fc) and its delegated certification authority (BR SSL Intermediate CA with hash algorithm SHA256 and fingerprint 37 7b 35 1c cb 87 a4 f5 f1 d3 99 78 56 13 15 cd 46 od 67 1a) by StartCom Root, during the period from 22nd of March of 2017 to 22nd of May of 2017.

In this period, CA-StartCom:

- Has disclosed its certificate practices and procedures and provided such services in accordance with its disclosed practices in the Certification Practices Statement version 3.1 (<https://www.startcomca.com/policy>) and their compromise to deliver the SSL certificates in accordance with the organization practices of Certification Authority Browser Forum (CA/Browser Forum), and provides these services to accomplish that practices.
- Has maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly collected, authenticated (for the registration activities), verified and performed by CA-StartCom.
 - The integrity of keys and certificates managed by CA-StartCom was established and protected throughout their life cycles.
 - Logical and physical access to CA systems and data was restricted to authorized individuals, and protected against not specified uses in the Business Practices Disclosure of AC-StartCom.
 - The continuity of key and certificate management operations was maintained.
 - CA systems development, maintenance and operations of CA-StartCom's systems were properly authorized and performed to maintain CA-StartCom systems integrity.
- The effective controls were maintained to satisfy the requirements of security in Networks and Certification Systems established by CA/Browser Forum.

In accordance with WebTrust for Certification Authorities — SSL Baseline Requirements with Network Security version 2.2 (<http://www.webtrust.org/principles-and-criteria/item83172.aspx>) that imposes CPA (Chartered Professional Accountant, Canada).

PricewaterhouseCoopers Auditores, S.L., Torre PwC, Pº de la Castellana 259 B, 28046 Madrid, España
Tel.: +34 915 684 400 / +34 902 021 111, Fax: +34 915 685 400, www.pwc.es

1

AC-StartCom's Management Responsibility:

AC-StartCom management is responsible for the preparation and presentation of its statement in accordance with the WebTrust Principles — SSL Baseline Requirements with Network Security version 2.2; providing the CA services included in the statement and establishing and maintaining effective controls over its CA operations.

Our Responsibility:

Our responsibility is to express an opinion on CA-StartCom management's statement, based on the procedures we have performed and the evidence we have obtained

We conducted our reasonable assurance engagement 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 Standard Board of the International Federation of Accountants.

Our test has been realized in accordance with WebTrust for Certification Authorities — SSL Baseline Requirements with Network Security version 2.2, established by the CPA, and includes:

- Obtaining an understanding about:
 - Business practices in relationship with the key and certification lifecycle management of CA-StartCom.
 - The integrity of keys and certificates managed by CA-StartCom.
 - Protection and privacy of Subscriber's data and Relying Parties.
 - Operations continuity of key and certification lifecycle management.
 - Development, maintaining and system operations of CA-StartCom.
- Selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business practices.
- Testing and evaluating the operating effectiveness of the controls.
- 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 qualified opinion.

Basis of qualified opinion

CA-StartCom does not comply with all the controls according to the Principles and Criteria WebTrust for Certification Authorities - Basic Requirements SSL version 2.2:

- Regarding to Principle 3. Environmental Security, the criterion where exception has been identified is:
 - 4- CA Environmental Security. The CA guarantee the Business Continuity Plan's development, implantation and maintenance.
It has evidenced that the business continuity plan defined hasn't been implemented.
- Regarding to Principle 4. Network and Certificate System Security Requirements, the Criteria where exceptions have been identified are:
 - 2.7 y 2.10- Trusted Roles, third parties delegated and system accounts. The CA has to maintain a procedure that assures the system passwords are renewal in each six months.
It has evidenced that there is no default password renew strategy maintained within the system.
 - 3.1- Audit, monitoring and alert. The CA guarantees the detection, monitoring and report any security-related configuration change to Certificate Systems.
It has evidenced that the existing system monitoring system cannot monitor, detect, and report any security-related configuration change to Certificate Systems.

In addition to the identified exceptions, two significant matters have been identified:

- On the one hand, StartCom has rehabilitated revoked certificates for Microsoft.
- On the other hand, StartCom has issued 4 test certificates to check the CT for types IV, OV and EV with a user that has assigned a super administrator role.

Auditor´s Opinion:

In our opinion, assertions by the management of the CA-StartCom in relation to its Practices as Certification Authority, regarding its practices as Certification Authority, except for the matter described in the Basis for Qualified Opinion, are properly formulated in all material matters, in accordance with the Principles and Criteria WebTrust for Certification Authorities - Basic Requirements SSL version 2.2 for the period from March 22, 2017 to May 22, 2017.

Other questions:

In order to comply with the controls mentioned in the "Basis of qualified opinion", after the period of this order, StartCom has developed a plan of corrective actions with the objective of solving the identified exceptions, having been implemented the majority of these actions.

Inherent Limitations

Because of the nature and inherent limitations of controls, error or fraud may occur and not to be detected. Furthermore, the projection of any conclusions based in our findings to future periods subsequent to the date of our report, is subject to the risk that the validity of such conclusions may be altered because of:

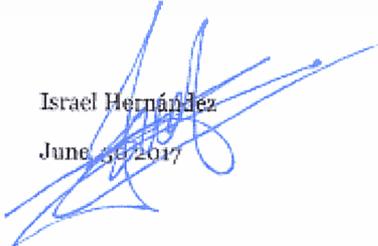
- Changes made to the system or controls;
- Changes in processing requirements;
- Changes required because of the passage of time; or
- Degree of compliance with the policies or procedures may alter the validity of such conclusions.

Exclusions

The WebTrust Seal of assurance for certification authorities on CA-StartCom website, 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 to provide any additional assurance.

This report does not include any representation as to the quality of CA-StartCom's certification services beyond those covered by the WebTrust Principles and criteria for Certification Authorities – SSL Baseline Requirements with Network Security version 2.2, nor the suitability of any CA-StartCom's services for any customer's intended purpose.

PricewaterhouseCoopers Auditores, S.L.



Israel Hernández

June 30, 2017



Assertion by Management of StartCom regarding its disclosure of its Certificate Practices and its controls over its SSL Certificates issuance provide as Certification Authority during the period from March 22, 2017 to May 22, 2017.

June, 30 2017:

Management confirms its understanding that your examination of our assertion related to Certification Authority of StartCom (hereafter "CA-StartCom") business practices disclosure and controls over its SSL Certification Authority operations during the period from March 22, 2017 to May 22, 2017, was made for the purpose of expressing an opinion on whether our assertion is fairly presented, in all material respects, and that your opinion is based on criteria for effective controls as stated in our assertion document. We are responsible for our assertion. In connection with your examination, management of AC-StartCom:

- Acknowledges its responsibility for establishing and maintaining effective controls over its SSL Certification Authority (AC-StartCom), including CA business practices disclosure (<https://www.startcomca.com/policy>), service integrity (including key and certificate life cycle management controls), and CA environmental controls.
- Has performed an assessment and believes that AC-StartCom SSL business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls met the minimum requirement of the criteria described in our assertion document during the period from March 22, 2017 to May 22, 2017.
- Has disclosed to you that there are no significant deficiencies in the design or operation of the controls which could adversely affect AC-StartCom's ability to comply with the control criteria related to AC-StartCom's CA SSL business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls, consistent with our assertions.
- Has made available to you all significant information and records related to our assertion.
- Has responded fully to all inquiries made to us by you during your examination.
- Has disclosed to you any changes occurring or planned to occur in controls or other factors that might significantly affect the controls, including any corrective actions taken by management with regard to deficiencies.

In management's opinion, AC-StartCom, in providing its SSL Certification Authority (CA) services, during the period from March 22, 2017 to May 22, 2017:

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines.
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly collected, authenticated for the registration activities performed by the CA-StartCom, and verified.

- The integrity of keys and certificates it manages was established and protected throughout their life cycles;
- Logical and physical access to CA systems and data was restricted to authorized individuals;
- The continuity of key and certificate management operations was maintained; and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

In accordance with the WebTrust for Certification Authorities – SSL Baseline Requirements v2.2 (<http://www.webtrust.org/principles-and-criteria/item83172.aspx>) by AICPA / CPA Canada.

Very truly yours,

Iñigo Barreira
CEO

A handwritten signature in black ink, appearing to read 'Iñigo Barreira', written over a horizontal line.