StartCom CA Limited

Independent's Practitioner Reasonable Assurance Report

pwc

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") related with the services of Code Signing realized to provide as Certification Authority services through the "StartCom Root" (StartCom Certification Authority CS with hash algorithm SHA256 and fingerprint 8e 20 7f 5d c0 a6 9a a3 37 65 8d 23 67 43 3e c2 7d 85 06 d0) and it delegated certification authority (CS Intermediate CA with hash algorithm SHA256 and fingerprint 5c b6 19 e3 08 4e 8f 1f 30 48 df c4 0a 5f 79 f4 a4 85 fa 95) 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 about privacy of information and their business practices about the lifecycle management of the Code Signing certificates (see the policy of Certification Practices version 3.1 published in their website https://www.startcomca.com/policy) and their compromise to deliver the Code Signing certificates in accordance with the organization practices of Certification Authority Browser Forum (CA/Browser Forum), and provides this services to accomplish that practices.

- Has maintained effective controls to provide reasonable assurance that:

    - Subscriber Code Signing information was properly collected, authenticated (for the registration activities), verified and performed by CA-StartCom.

    - The integrity of keys and Code Signing certificates managed by CA-StartCom was established and protected throughout their life cycles.

    - The authorization request of Code Signing and the timestamp are properly authenticated.

    - The Code Signing Certificates and the timestamp are issued are not valid for a period longer than the time specified by CA / Browser Forum.

In accordance with WebTrust for Certification Authorities — Publicly Trusted Code Signing Certificates Version 1.0 (http://www.webtrust.org/principles-and-criteria/item83172.aspx) that imposes CPA (Chartered Professional Accountant, Canada).

R. M. Madrid, hoja 87.250-1, folio 75, tomo 9.267, libro 8.054, sección 3ª
Inscrita en el R.O.A.C. con el número S0242 - CIF: B-79 031290

AC-StartCom's Management Responsibility:

CA-StartCom management is responsible for the preparation and presentation of its statement in accordance with the WebTrust Principles — Publicly Trusted Code Signing Certificates Version 1.0; 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 AC-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 — Publicly Trusted Code Signing Certificates Version 1.0, established by the CPA, and includes:

- Obtaining an understanding about:
    - Business practices in relationship with the key and certification lifecycle management of Code Signing certificates of CA-StartCom.
    - The integrity of keys and certificates of Code Signing managed by CA-StartCom.
    - Protection and privacy of Subscriber's data and Relying Parties.
    - Operations continuity of key and Code Signing certification lifecycle management.
    - Development, maintaining and system operations of CA-StartCom.
- Selectively testing transactions executed in accordance with their disclosed business practices about the privacy of the information and 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 — Publicly Trusted Code Signing Certificates Version 1.0:

- Regarding to Principle 2: Code Signing Service Integrity, the Criteria where exceptions have been identified are:

    - 5.5- Certificate Revocation and Status Checking. The CA has to guarantee the revocation of the certificates through a correct validation process.
      It has evidenced that testing certificate was issued during the audit period which lacked regulated request and validation process.
      In addition, regarding to StartCom's revocation request validation process, an individual can request for revocation as long as his client certificate is valid, without provide any identity documents of the organization.

    - 7.4- Data Records. The CA has to guarantee the registry of the IP connection.
      It has evidenced that the timestamp server cannot record the connecting IP.

    - 9.2. And 9.3- Timestamp Authority, Signing Services, and Private Key Protection. The CA has to guarantee that the Private Key of timestamp service can be exported and also, the private key has to protect through a hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
      It has evidenced that the private key of timestamp service cannot be exported. Also, the private key was protected by Microsoft built-in certificate protection mechanism.

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 — Publicly Trusted Code Signing Certificates Version 1.0 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 — Publicly Trusted Code Signing Certificates Version 1.0, nor the suitability of any AC-StartCom's services for any customer's intended purpose.

PricewaterhouseCoopers Auditores, S.L.

Israel Hernández

June 5, 2017

StartCom®

Assertion by Management of StartCom regarding its disclosure of its Certificate Practices and its controls in relation to operations as a Code Signing Certification Authority Services 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 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 Certification Authority (AC-StartCom) of services of code signing certificates, 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 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 business practices disclosure, service integrity (including key and code signing certificates lifecycle 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 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 services of certification authority 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.

StartCom®

- The integrity of keys and code signing 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 – Publicly Trusted Code Signing Certificates v1.0 (http://www.webtrust.org/principles-and-criteria/item83172.aspx) by AICPA / CPA Canada.

Very truly yours,

Iñigo Barreira
CEO