StartCom Remediation Plan

Oct. 14th, 2016

Introduction

In line with the plan that was presented to Mozilla representatives for their advice and comment, Qihoo 360, the controlling shareholder of WoSign, will separate WoSign and StartCom, so that each company will be independent of each other.

Following the separation, StartCom will be owned directly by Qihoo 360 and will have its own separate management/legal structure, systems and operations.

The tasks to separate the companies will take into account these three main points:

(1) Management and legal structure separation
(2) Operations separation
(3) Systems separation

Those actions and steps taken will be audited accordingly by a WebTrust qualified auditor. Mozilla can name a specific WebTrust auditor and StartCom will reflect the changes done.

(C) 2016 StartCom CA Limited

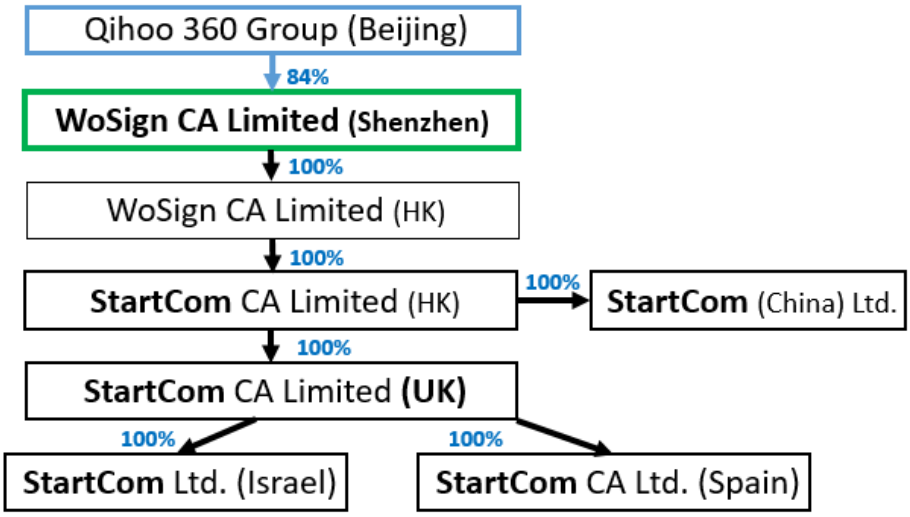
Actions

These are the actions planned and scheduled for the changes in StartCom.

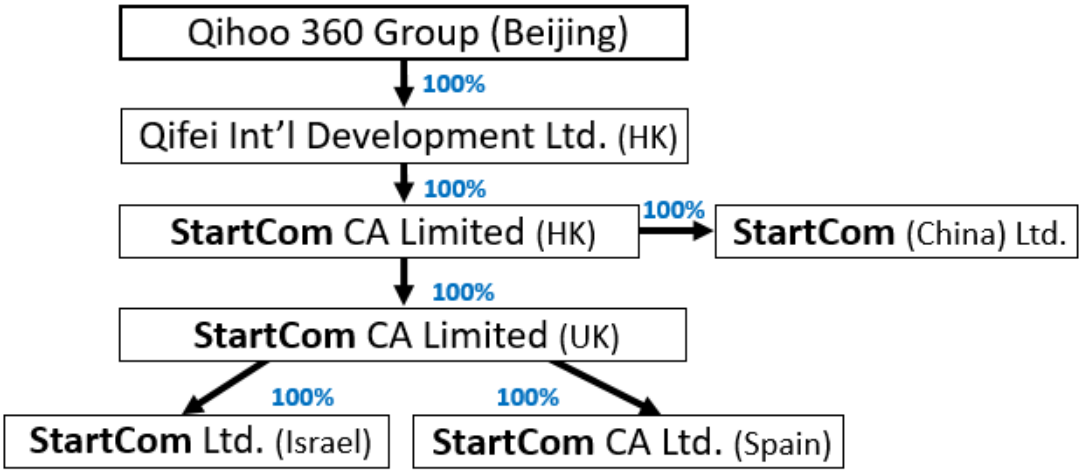
1. Legal Structure and management separation

Qihoo 360 will completely separate the legal structure of WoSign and StartCom so that StartCom is a directly owned subsidiary of Qihoo 360 and has no legal ownership by WoSign.

Here is current StartCom structure:



StartCom will separate from WoSign and become Qihoo 360 100% subordinate company, the StartCom structure will be:



(C) 2016 StartCom CA Limited

The StartCom Hong Kong shareholder change is expected to be finished before Oct.30, 2016.

The director of those StartCom companies will change from Gaohua Wang (Richard Wang) to Tan Xiaosheng (Qihoo 360), Yang Qing (Qihoo 360) and Inigo Barreira (CEO of StartCom), so that Richard Wang won´t have any relationship with these companies.

Mr. Tan Xiaosheng is named Chairman of StartCom, effective since October 5th 2016.

Mr. Inigo Barreira was named CEO of StartCom since September 19th 2016.

2. Operations separation

Basically any previously shared functions (where they existed) will be separated including the validation team, customer service team and technical support team.

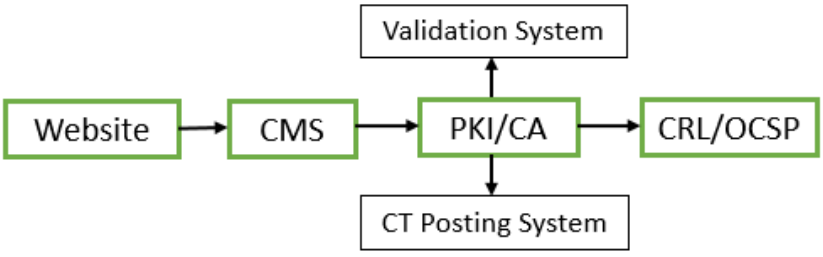
StartCom will have their own teams and all the operations will be run by StartCom employees only:

- There are a validation team, a customer service team and a technical support team that will work from China and UK. New people will join these teams from Spain next year.
- During the rest of 2016, the HR and accounting departments will be done by Qihoo 360; StartCom will hire people for managing these departments starting in 2017.
- StartCom China will move to Qihoo 360 Shenzhen office by Oct. 30th 2016.
- Qihoo 360 R&D team will take control over the StartCom website, CMS and PKI, CRL/OCSP system, TSA system, Validation system, CT posting system, etc. as a short term solution from Oct.17th 2016, StartCom will have its R&D team to take over the responsibility in 2017

3. System separation

There are 4 systems, all of them, regarding infrastructure and communications, are managed and controled by Qihoo 360 team since Dec. 22th 2015. The Startcom website is hosted in Qihoo 360 USA IDC, the CMS/PKI/CRL/OCSP system is hosted in Qihoo 360 China IDC.

Here is the diagram for the whole system



(C) 2016 StartCom CA Limited

These are the next actions:

Website

Current status

The StartCom website uses and works with the same logic than the old one, before the acquisition. But it was re-designed and updated the code when Wosign acquired StartCom to provide more functionality and ease of use.

The website is hosted in a separate server and use another database, nothing related to WoSign. They are hosted in Qihoo 360 IDC in the US.

Next steps

Qihoo 360 code and security team will audit internally and check and review the code and if necessary, will re-code it again adding an enhanced security.

This task should be finalised by December 31st, 2016.

CMS

Current status

Similar to the website, the CMS system has the same logic and procedures as the old StartCom CSM solution, but was revised and then redesigned and coded again by WoSign R&D team.

The CMS system is hosted in a separate server and uses another database, withnothing related to WoSign. They are hosted in Qihoo 360 Headquarters, Beijing.

Next steps

Qihoo 360 code and security team will audit internally and check and review the code and if necessary, will re-code it again adding an enhanced security.

This task should be finalised by December 31st, 2016.

PKI system

Current status

The StartCom PKI system was cloned from the WoSign one. Since the acquisition only a new intermediate CA was created.

Both companies have HSMs for them, hosting their keys and doesn't share anything. Just use the same code as is an in house development by the Wosign R&D development

(C) 2016 StartCom CA Limited

Next steps

StarCom proposes 2 solutions based on timing

Short term

StartCom will go back and recover the "old" code (previous to the acquisition) and this code will be reviewed and update to comply with the international standards defined by IETF, CAB Forum, etc. This task will be accomplished by Qihoo 360 security team.

This task should be finalised by December 1st, 2016.

Mid term

Meanwhile, StartCom will acquire a third party PKI software from accredited providers and will start the integration with its Website and CMS systems. Once the complete integration is finalised, the "old" PKI system will be switched off and everything will run with the new one. In any case, there will be some time in which both systems will be running in parallel to adjust some possible issues.

This task is estimated to be finalised by February 2017.

OCSP/CRL

Current status

The StartCom OCSP/CRL system was cloned from the WoSign one. It´s hosted in Qihoo 360 IDC in China and use Akamai CDN for distribution outside China, using Qihoo 360 CDN for distribution in China.

Next steps

Qihoo 360 code and security team will audit internally and check and review the code and if necessary, will re-code it again adding an enhanced security. Will also develop the interface for providing the PKI data to the OCSP/CRL system

This task should be finalised by December 1st, 2016.

So, in summary, all the system separation tasks will be done before the end of the year 2016, except the integration with the third party PKI software, that will take more time.

At the same time, a full review of all StartCom documentation, mainly CP/CPS, will be reviewed to meet the requirements set by the CA/B Forum (Baseline Requirements and EV guidelines) and those policies set by the browsers in their root programs with the same end date, 31st December 2016.

4. CT logging

(C) 2016 StartCom CA Limited

StartCom started to log all issued SSL certificates to publicly know CT log servers on March 26th, 2016, and fixed the mis-loging bug in July 6th 2016.

For the EV SSL certificates, StartCom is using the following CT log servers:

https://ct.googleapis.com/pilot

https://ct.googleapis.com/aviator

https://ct.googleapis.com/rocketeer

https://ctlog.api.venafi.com

For non EV SSL certificates, and due to the number of certificates StartCom issues, StartCom is using the following.

https://ct.googleapis.com/pilot

https://ct.googleapis.com/aviator

https://ct.googleapis.com/rocketeer

https://ct.startssl.com

https://ctlog.wosign.com

StartCom and WoSign CT log servers have been quanlifed by Google and will be include in Chrome release 54. StartCom will try to use other CT log servers with enough capacity for all issued certificates.

Thanks.

StartCom CA Limited

(C) 2016 StartCom CA Limited