Symantec Response to Further Questions from Mozilla – 15 May 2017

RAs and EV ---------- 1) Did any of the RAs in your program (CrossCert and co.) have the technical ability to independently issue EV certificates? If they did not, given that they had issuance capability from intermediates which chained up to EV-enabled roots, what technical controls prevented them from having this capability?	Yes, the former TLS RAs had the technical ability to cause issuance of EV certificates. As a general practice, Symantec conducted EV authentication for both retail certificate orders and in Enterprise RA accounts for former TLS RAs. In 4 cases, between Jan 2014 and Feb 2015 two of these former TLS-RAs conducted the EV domain validation for Enterprise RA accounts: CertSuperior had validated one organization that had two domains. Symantec has confirmed that each of these validations met the EV authentication guidelines when completed. A total of 3 certificates were issued and all have expired. Certisur had validated two organizations each with one domain. Symantec has confirmed that each of these validations met the EV authentication guidelines when completed. The first organization issued 2 certificates and all have expired. The second organization issued 22 certificates, 6 have expired, and 14 remain active. In each of these cases, the organizations and domains were subsequently revalidated by Symantec personnel between Jan 2015 and Mar 2016. In Dec 2014 CrossCert issued 1 EV certificate that did not meet the EV authentication guidelines (not included in the 4 above); this certificate is expired; this was issued as part of a documented technical support case; the customer was aware of the issuance as part of the case; and it was done to help diagnose an issue where sessions were failing and suspected to be due to a change in the EV-enabled subCA used for issuance.
RAs and EV ---------- 2) We note that all four RAs advertised EV certificates on their websites during 2016. If they did not have direct EV issuance capability, by what mechanism did they provide EV certificates to their customers, and what validation (if any) did Symantec do of data provided by the RAs?	All former TLS RAs were also authorized resellers of Symantec certificates. With the limited exceptions in #1 above, when customers ordered EV certificates through these partners, their submitted certificate request information was passed to Symantec to process directly. In these cases, the partner did not supply information to Symantec or perform any validation work before the information was submitted to us.
Issue Y ------- 3) Does Symantec agree that "VeriSign Class 3 SSP Intermediate CA - G2" and "Symantec Class 3 SSP Intermediate CA - G3", can issue certs which are trusted for SSL/TLS in Mozilla products (by chaining up to "VeriSign Universal Root Certification Authority") and yet do not have BR audits?	These two subCAs (1 & 2) and a third one, the Symantec Class 2 Public Primary Certification Authority - G6 (3), are 3 intermediate CAs for the Non-Federal Shared Service Provider program. Below are the details and plans for all three. (1 & 2) These two Class 3 SSP CAs chain to both the VeriSign Universal Root Certification Authority, which is trusted by Mozilla for websites, code signing and email, and to the Federal Bridge CA 2013, soon Federal Bridge CA 2016. The subCAs under these are dedicated to individual government contractors or agencies. All of these subCAs operate fully within Symantec's environment. While the subCAs are unconstrained, the platform from which they issue certificates has system controls limiting their usage. Certificate

profiles solely under the control of Symantec limit issuance by each subCA to specific key usage and extended key usage. In all cases but one (see below), those system controls prevent TLS Server Authentication issuance. Further, these certificate profiles assert SSP policy OIDs and do not include BR policy OIDs.

In the case of the one Non-Federal Shared Service Provider customer with the ability to issue certificates with TLS Server Authentication (from the CSC Device CA – G2 and the CSRA FBCA C3 Device CA, both named in our NFSSP WTCA audit), they previously issued a total of 33 domain controller certificates. Four of these are currently valid and 29 are expired or revoked. The customer is a government contractor, the use case supports controlling network logon and access to resources.

No certificates in the SSP contain the CABF BR policy OID. They only contain our SSP policy OIDs, 2.16.840.1.113733.1.7.23.3.1.8 or 2.16.840.1.113733.1.7.23.3.1.36. None of these certificates contain domain names or TLDs.

Based on the system controls, the policy OIDs, and the intended policy-constrained usage of these subCAs, they have been subject solely to WTCA audits but not WTBR audits.

(3) Our Class 2 SSP CA is signed by the Symantec Class 2 Public Primary Certification Authority - G6. The latter is trusted by Mozilla for email. This is subject to WTCA audits.

We agree with Mozilla that legacy Federal PKI and web PKI are a complicated mix.

Since SSP certificates fully function under the Federal Bridge CAs and the Federal Government Common Policy CA, our Class 3 Non-Federal SSP intermediates do not need trust from the Universal Root. In addition, the Class 2 SSP CA no longer needs trust under the Symantec Class 2 root. As a result, we are in the process of privatizing the trust chains that support our Non-Federal SSP program overall.

To simplify these trust chains, we have created two private roots for the three Non-Federal SSP subCAs. We have signed our Non-Federal SSP intermediates with these new private roots, we are deploying them in place of the public root versions. We will revoke the public versions of these subCAs that are signed by roots trusted by Mozilla on May 24, 2017. This has been communicated to customers and was reviewed during the most recent FPKI PA call.

For the domain controller case above, we have suspended the ability for any Non-Federal SSP customer to issue new domain controller certificates until we deploy the private trust replacement sub-CAs.

Issue Y ------- 4) These two intermediates have a number of sub-intermediates. Does Symantec agree that not all of these sub-intermediates are within the scope of even Symantec's NFSSP Webtrust for CAs audit? If so, how many are in scope and how many are out of scope? If they are all in scope, why are they not listed in the audit document?	With respect to these 8 sub-intermediates: https://crt.sh/?id=19602740 https://crt.sh/?id=19602709 https://crt.sh/?id=19602733 https://crt.sh/?id=19602720 https://crt.sh/?id=19602670 https://crt.sh/?id=19602679 https://crt.sh/?id=19602705 https://crt.sh/?id=19602730 Of the above, only State of Florida AHCA Medium Assurance CA (https://crt.sh/?caid=18731) has ever issued certificates. That CA issued 27 certificates – 19 are OCSP responder certificates automatically generated by our systems; the last of the 8 TLS certificates expired June 18, 2014. Seven of these 8 expired in June and July 2013, 3 of the 7 were revoked prior to expiration. Our Non-Federal SSP customer CA list and the scope of certificate sampling for our audit were based on CAs that had or issued valid certificates during the period. We noted these CAs in a footnote to our Non-Federal SSP audit. Annually, we determine CAs that require sampling versus CAs that are idle using an inactivity report. Regardless of activity, idle CAs are included in WebTrust control objectives that prove that the CA was properly managed and secured. Our auditors state a CA list in the scope of our audits for those CAs that had or issued valid certificates during the audit period. We believe that having our audits enumerate all CAs capable of issuance, regardless of whether or not they are used, ensures completeness of coverage of the audits, and that's something we intend to do going forward. Updating the industry-wide standards for audit scope along these lines was a key topic in a recent WebTrust working group meeting. Per your prior request, we are preparing our publicly trusted PKI map that will answer these types of questions for all of our public CAs. The elements of the map will include: 1. The list of all publicly trusted Roots and SubCAs 2. Identification on whether through KU/EKU, browser policy, or Symantec system controls these Roots and SubCAs are capable of serverAuth and EV certificate issuance. 3. Based on these controls, our assessment of what audits these Roots and SubCAs should be subject to, and the status of those audits. We expect to publish the full publicly trusted PKI map once we have verified all of the information.

Issue Y ------- 5) A statement from Symantec suggests that customers of your NFSSP program can perform RA duties for the issuance of certs for Windows domain controllers and those RA activities are outside the scope of the audit entirely. Is that correct? Please list all companies or organizations which can issue publicly-trusted SSL/TLS certificates with no audit oversight.	Please see our response to question #3 where this is answered.
Issue Y ------- 6) "VeriSign Universal Root Certification Authority" is EV-enabled. Are there any mechanisms, technical or otherwise, which prevent NFSSP customers from issuing EV certs by including the Symantec EV OID?	Yes. System controls prevent issuance of EV certificates for all subCAs in the Symantec NFSSP program. All NFSSP certificates are issued based on a profile defined by Symantec. NFSSP customers have no control over any certificate extension content except subject alternative name and only indirectly via common name. Customers may only elect to operate profiles as defined in Appendix A of our NFSSP CPS. The Device profile in table A.5 indicates the list of CP OIDs we permit (which does not include EV OIDs); this Appendix references Common Certificate Policy OIDs, as documented in Worksheet 7 [1], as also permitted.
Issue Y ------- 7) Does Symantec agree that Issue Y is very serious? What are Symantec's plans to remedy this? Why have they not been communicated up to now? When will they be executed?	Yes, we take Issue Y very seriously. We have been conducting a thorough review of the NFSSP program. Please see our response to question #3 for the summary and action plan.
Issue L ------- 8) During the approximately five years that Symantec cross-signed the Federal PKI, thereby making any certificate within it have a path to trust in Mozilla browsers, which of the following best represented Symantec's understanding of the situation: a) Symantec didn't realise that your actions had the effect of making the entirety of the FPKI trusted in Mozilla browsers; or b) Symantec knew that your actions had the effect of making the entirety of the FPKI trusted in Mozilla browsers and didn't realise the implications for your own audits and disclosures and the WebPKI; or c) Symantec knew that your actions had the effect of making the entirety of the FPKI trusted in Mozilla browsers and did realise the implications, but didn't think it was necessary to tell Mozilla about it?	The initial cross-signing of the FPKI was done in 2009 prior to our acquisition of the business from VeriSign in 2010. We began working with the FPKI in 2014 to determine whether this cross-signing was actually required and the effect that its removal would have on critical infrastructure. This remained unconfirmed until 2016. It was resolved with the expiration of the cross-signing in mid-2016.

Issue L ------- 9) Do you agree that, during the period of time that Symantec cross-signed the Federal PKI (Issue L), it was technically possible for issuers inside the FPKI to issue EV certs by inserting Symantec's EV OID?	We cannot answer this definitively because we only support a portion of the Federal PKI. In the case of the Symantec-operated subCAs in the Federal and Non-Federal SSP programs, system constraints prevented the insertion of additional (including EV) OIDs. The FPKI Policy Authority has a procedure to monitor profiles and annually requires all participants to submit sample certificates for each enabled SSP profile. As a result of the strong oversight by the PA of SSP submissions, the probability of the PA detecting an EV enabled certificate being produced by a device profile is very high.
Other ----- 10) If, in the Symantec Issues list or any other document relating to this matter we may publish in future, we have drawn a conclusion or inference about Symantec's PKI, actions or behaviour which is incorrect, we expect you to draw that to our attention, even if the truth is not as favourable to Symantec. Are there any incorrect inferences or conclusions in the Issues List which need to be corrected?	In Issue Q: regarding unregistered domains, you commented: “Mozilla isn't aware that Symantec has previously made disclosure of this mis-issuance.” >> These certificates were included in the disclosure in April 2016 at the conclusion of our investigation. In Issue Q: you asked, “Is a CA allowed to rewrite its management assertions during the audit process so as to include as "known" any problems found? Would this make the difference between failing and passing an audit?” >> We believe there’s a misunderstanding from our earlier responses. See more details in the response regarding audits below. In Issue Q: you stated, “It is also not clear whether the disclosure in the cover letters excuse the absence of qualifications related to GeoRoot and the RA program in these audits.” >> Our auditor’s scope and opinion did not include the results of third party audits, only Symantec’s process regarding requesting and following up on any gaps in those third party audits. We provided the cover letters to ensure transparency related to the issues we had encountered with the third party audits. This is an example of the type of communication the community has asked us for. In Issue T: you stated, “However, the determination of deficient validation was made based on the RAs own logs of activity, which may themselves be suspect given some of the audit deficiencies found at these RAs.” >> In the case of CrossCert (the specific subject RA in issue T) we have completely revalidated the orders, not relying on previous work. Issue Y: You state, “No Response” >> See answers to questions #3, #4, #5, #6, #7 above.
Other ----- 11) As requested in an email to Steve Medin on 5th of May and noted again in an email to	As per Baseline requirements, Aetna and UniCredit were operating as a CA in the context of section 8.6, and they themselves were obligated to publish audits. As a reminder, both the Aetna and UniCredit ICAs were revoked (11/30/2016 and 10/18/2016,

Quentin Liu on 10th May, please provide copies of all audits of any type relating to the Aetna and UniCredit GeoRoot intermediates. You may attach them to a Bugzilla bug or place them in another public location and provide the URL.	respectively) so there should be no existing trust issues with certs under those ICAs. Symantec has published the Aetna audits on CCADB. Symantec had asked for, but had not received an audit from UniCredit, so UniCredit has no completed audit to share. They have an internal use only assessment and an ETSI audit performed by an auditor. We could not determine if such auditor was ETSI approved. There is no audit to release.
Audits ------ Please explain how the Management Assertions for your December 2014 -> November 2015 audits contain documentation of issues ("Failure to maintain physical security records for 7 years", "Failure to review application and system logs" and "failure to refresh background checks every 5 years") that, according to you, were only discovered in January or February 2016[3]. Is it not the case that you submit Management Assertions to your auditor and they then opine upon the correctness of those assertions? What is the "last change date" of those management assertions? What point in the audit cycle does that date correspond to?	We believe there is a misinterpretation of some of our prior responses related to the time lag between audits being completed and the reports being published. The only relevant edits we have made to the drafts of our audit reports have been to correct inaccuracies and to provide the management responses to issues identified during the audit (e.g to ensure the accuracy of the descriptions of any root causes and the status of remediation).

[1]: https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000Gmi3AAC&field=File__Body__s