Symantec Second Response to Mis-Issuance Questions – February 12, 2017

Based on our investigation of CrossCert, we have concerns due to (1) demonstrated non-compliance with processes and controls, (2) assertions of third party auditors that need far greater oversight than we previously expected, and (3) the fact that these issues have enabled cases of certificate mis-issuance. As a result, we have made the decision to terminate our partner RA program. We will continue to work with select partners that have local market contacts and expertise to facilitate an interface with customers and collection of relevant documentation, however Symantec personnel will validate 100% of all asserted identity data and control certificate issuance going forward. We have communicated this change to each of our RA partners, we are finalizing a transition plan, and intend to implement that transition quickly. In addition, to alleviate any concern by customers or relying parties on the integrity of the certificates issued by these RA partners, Symantec will review the validation work of 100% of issued certificates and revalidate any where we identify any deficiency. Certificates issued with deficient validation will be replaced and revoked. Our work will be included in scope of our next WebTrust audits.

Question	Symantec Response

• You say that one of your WebTrust audited partners issued these certificates. Is this partner Korea Electronic Certification Authority, Inc. (”CrossCert”)?
• If yes, according to the audit report here https://cert.webtrust.org/SealFile?seal=2168&file=pdf this partner is allowed to use the following three issuing certificates from Symantec:
  ○ VeriSign Class 3 Secure Server CA - G3
  ○ VeriSign Class 3 International Server CA -G3
  ○ Symantec Class 3 Secure Server CA - G4
• However when I look at all the "test" certificates I find these issuers:
  ○ 4 issuer= /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3
  ○ 99 issuer= /C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4
  ○ 11 issuer= /C=US/O=thawte, Inc./CN=thawte SSL CA - G2
	• Symantec authorized CrossCert to issue certificates from each of the identified CAs.
	• The list of CAs in the audit was produced by CrossCert and given to E&Y KR as the scope to audit. It was not given to E&Y by Symantec.
	• E&Y KR initially stated that CrossCert did not fully disclose the list of CAs. E&Y KR later stated that CrossCert provided a list of all their issuing CAs but reduced the list of issuing CAs in scope of sampling for budgetary reasons.
	• Due to these conflicting statements and further discoveries explained below, Symantec will no longer accept audits from E&Y KR.
	• Symantec is terminating RA delegation to CrossCert. Symantec’s Authentication team has taken over validation since January 19, 2017 and will continue as the only RA responsible for verification work resulting in issuance of new and replacement certificates to CrossCert customers.

The six "false positive" certificates appear unremarkable except for the coincidence of including the word "test". If CrossCert can't produce documentation to show these were validated properly, it seems likely that many or even all certificates which Symantec had believed were validated by CrossCert in fact lack such documentation. Is that not so?	• We have confirmed that there are deficiencies in the documentation and audit trails for validation performed by CrossCert. We are terminating RA delegation to CrossCert. Further, Symantec’s Authentication team is re-validating 100% of certificates issued by CrossCert using local language expertise. The timing of this is dependent on staffing Korean speakers, following our strict onboarding procedures, and completing the re-validation of all currently valid certificates. Our work will be included in the scope of our next WebTrust audits.
It had been my assumption, based on the CPS and other documents, that CrossCert was restricted in their use of Symantec's issuance function to C=KR, this is cold comfort for practical purposes in the Web PKI, but it would at least help us to scope any damage. The existence of certificates with C=BD in this list shows my assumption was wrong. How (if at all) can an outsider determine if in fact CrossCert caused issuance of a Symantec certificate? Prior to Andrew's report what _mechanical_ constraints on CrossCert's issuance were in place, in particular any beyond those which were applied to Symantec's own issuances? For example, would it have been	• CrossCert’s CPS at table 5 in section 3.1.1 at http://www.crosscert.com/symantec/certificationeng.pdf states that Country will contain “KR” or not be used (in usages other than TLS Server Authentication). • We have confirmed that CrossCert has issued certificates that contain a country code other than KR. • CrossCert does not operate a subordinate CA that externally distinguishes their issuance. • Our first question response document described our compliance checks prior to and after issuance. The 39

possible for them to cause issuance of a 5-year cert? A SHA-1 certificate? To choose specific serial numbers?	month limit, SHA256 requirements, and other technical conformity checks are enforced prior to issuance and checked post-issuance. These checks cannot be overridden. These checks are replaced by multiple engineering and compliance team checks in the case of manual key ceremony signing events. Serial numbers are generated automatically after the RA causes issuance of the certificate using a CSPRNG with appropriate entropy.
Since we have every reason to imagine that some (or even all) of the affected certificates were issued in good faith to legitimate subscribers, it would have been nice for Symantec to alert the subscribers when their certificates were revoked. Did Symantec do this? If not does Symantec have the capability to contact these subscribers itself (e.g. email addresses, phone numbers)? If not, does Symantec contractually require of RA partners that they provide a capability for Symantec to contact their subscribers, or relay a message chosen by Symantec on their behalf?	• Yes, these customers were notified. • CrossCert was alerted that we intended to comply with the 24 hour revocation requirements of the BRs. • In places where we rely on the local language skills and business relationships of our RA partners, we communicate to our partner and they notify their customers.
Although BR 5.4.1 says that these records are to be kept by the CA and each Delegated Third Party the obligation is on the CA (here, Symantec) to make the records available to their auditors. Is it in fact the case that this investigation is the first time Symantec has asked Crosscert for such records? Wasn't Symantec concerned that KPMG (in a routine audit) might ask to see these records but they didn't have them? Might not other RA partners be affected similarly?	• CrossCert is a WebTrust audited delegated third party required to make their delegated record keeping available to their auditor. • Symantec complies with BR 5.4.1 by delegating CrossCert to perform 2(c) for the certificates they issue. All other 5.4.1 event recording is performed by Symantec's software, hardware, or Trusted Role personnel using software, hardware, document, or paper-based methods. • Symantec relied upon CrossCert's unqualified WebTrust audit as a statement of compliance, and upon E&Y Korea's opinion as meeting WebTrust objectives.
As Symantec will know from its own experience, audits have not proved to be sufficient for detecting systematic non-compliance by CAs. What measures _beyond_ the Webtrust audit did Symantec have in place to detect non-compliance by an RA partner?	• To the extent that we relied on RAs for authentication and verification, we relied on their independent WebTrust audits to detect non-compliance. • We employ automated compliance checking prior to and after issuance. Further, we have deployed support for, and honor Certification Authority Authorization across all systems to put control of authorized CA's in the hands of customers, we log all publicly trusted certificates to Certificate Transparency Logs, and we have created a monitor to put visibility in place for all customers to enable detection of suspect certificates.
Did Symantec do any additional training for RAs regarding the issuance of test certificates after the last incident? If not, why not? Did Symantec believe that it was very unlikely for RA personnel to make the same mistakes or have the same misunderstandings of what was appropriate as Symantec's personnel?	We did not do additional training for RAs regarding the issuance of test certificates. However, we put in place a programmatic control to identify and flag likely test certificates by screening all certificates, including those processed by RAs. In the case of CrossCert, our audit logs show that CrossCert overrode the compliance failure flags. CrossCert did not consult with Symantec on the significance of the compliance failure flags or the decisions to override the flags for any of the certificates.
Is your understanding that, when WebTrust audits are sampling, they sample only certificates issued during the review period? Or should they be sampling certificates issued during the entire period covered by the audit? If the latter, did	Symantec's experience and expectation is that WebTrust audits include a representative sample of certificates issued during the audit period of time. Symantec relies on WebTrust audits to confirm that proper controls were in place governing certificate

their sampling (3%, isn't it?) hit any Category C certificates? How many certificates were in the sample pool?	issuance during a specific period in time. The last E&Y KR audit did not include verification of the issuance of the Category C certificates since they were issued in an earlier period. We recently learned that E&Y's recent sample size was 25 of the certificates issued in the last audit period. The 3% review is related to internal self-audit under BR 8.7.
To be totally clear: would it be correct to say that up until this point, examining WebTrust audits was the only mechanism that Symantec used to _check_ the conformance of their RAs to Symantec's CP/CPS and other requirements? (I see you give them software, and docs, and training, but was this the only _checking_ mechanism?)	To the extent that we rely on RAs for authentication and verification, we relied on their independent WebTrust audits to detect non-compliance. Technical requirements such as ensuring minimum key lengths, blocking SHA1, and other areas of technical conformity are subject to several additional controls.
Is there any reliable programmatic way of determining, looking only at the contents of the certificate or certificate chain, that a certificate was issued by CrossCert personnel using their processes, as opposed to by Symantec personnel or by another RA?	No. The most viable check would be to examine certificates with a KR country code, however while CrossCert was the only Symantec RA in KR, they have not been the exclusive source of enrollments in KR. Such a search would not distinguish KR certificates validated by CrossCert from those that Symantec processes directly. In any event, we are revalidating every valid certificate issued by CrossCert.
Given the many issues very clear from CrossCert's CP/CPS, and the many audit issues disclosed in CertSuperior's report, I'd like to request that you also disclose the CP/CPS for these CAs. For example, CertiSign's CP/CPS is not immediately obvious to me as to what Symantec was relying on EY to audit.	http://vtn.certisign.com.br/repositorio/politicas/DPC_da_Certisign.pdf https://www.certsuperior.com/docs/CPS_Final_2016_version_4_1_0.pdf
To echo Gerv's remarks, the statement Symantec issued for the previous misissuance [1] stated: "Symantec has updated its internal policies and procedures to strongly reinforce that all test certificates must follow the same fulsome authentication procedures as commercial certificates." Section 9.8 of the Baseline Requirements, v1.4.2 states "For delegated tasks, the CA and any Delegated Third Party MAY allocate liability between themselves contractually as they determine, but the CA SHALL remain fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated. " 1) Does Symantec believe that the original statement is sufficiently clear that it was limited solely to Symantec's role in validating, and did not extend to that of Delegated Third Parties?	There were no limits to the spirit of the statement we made. Practically, as stated previously, in 2015 we identified internal Symantec procedures for handling certificates used for internal testing purposes, we changed those procedures, and we retrained the individuals who had used those procedures. Separately, we continued the existing practice of requiring training of our RA partners – that training never justified publicly trusted certificates used for testing. We believed that this training was clear to all partners.
2) Did Symantec management believe it was not necessary to notify and inform its Delegated Third Parties about the need and significance to conform to Symantec's CP and CPS, and of the necessity of ensuring that all issued certificates - regardless of mechanism - must follow the same fulsome authentication procedures?	Software controls, training, documentation and annual exams reinforce these concepts. Audits we have received document disclosure of the RA's CPS. Each RA's CPS operates under the STN CP and is audited for conformity to CABF BR.
3) The most recent version of Certisign's CP/CPS that I'm able to publicly confirm is	Yes, that is the correct CPS and it implements the STN CP.

http://vtn.certisign.com.br/repositorio/politicas/DPC_da_Certisign.pdf , which is dated 2012. Is this the correct CP/CPS?	
4) Can Symantec confirm that this is the CP/CPS that was audited?	Yes, that is the correct CPS. This CPS implements the STN CP.
5) Does Symantec believe that this CP/CPS is consistent with Symantec's update CP and CPS documents updated in response to the previous misissuance?	Changes to internal procedures did not extend to the STN CP and CPS.
6) Does Symantec believe that the audit letter, indicated in [2], which clearly indicates that the effective criteria were based on "SSL Baseline Requirements Audit Criteria, Version 1.1", available at [3], represents a sufficient demonstration of conformance to Symantec's CP/CPS?	No. E&Y BR produced two deficient letters regarding the 2014 and 2015 Certisign audits. Initially we received a letter that stated a January 1, 2014 to December 31, 2014 audit period in its introduction and a January 1, 2014 to December 31, 2015 audit period in its conclusion. The letter appeared to cover a two year period. We asked for clarification multiple times. That clarifying letter stated a 2015 audit period. E&Y BR does not meet our requirements for RA audit quality, timeliness, and responsiveness to our demands. Symantec will no longer accept audits from E&Y BR should we have a future need for in-market audit support.
7) Does Symantec believe that the audit letter, indicated in [2], conducted by Ernst and Young Brazil, conforms with the professional obligations with respect to WebTrust licensing, and Symantec's obligation to ensure said compliance as part of its Delegated Third Party conformance to the Baseline Requirements' audit standards? Specifically, the requirement to use "WebTrust for CA - SSL Baseline with Network Security 2.0" for all audits whose periods begin after 1-Jul-14, which EY Brazil demonstrably did not follow?	No. E&Y BR's letter incorrectly specified v1.1 due to the date range error above. The updated audit letter documents failure to use the proper audit specifications for calendar year 2015.
Regarding Certsuperior: Symantec has indicated that the 2016 audit of Certsuperior was qualified, as demonstrated in [4]. During Symantec's previous misissuance event, Symantec noted that: "We have also enhanced our compliance function by consolidating all compliance activities into a single group reporting directly to the head of our Website Security business unit. This change was made in January 2016; this new compliance structure includes enhanced identification, tracking, prioritization and resolution of compliance-related updates, which will help ensure that CA/Browser Forum rule changes are effectively implemented." 8) Was Symantec's compliance group involved in reviewing the qualified audit report findings?	Yes. Upon receipt of the qualified Certsuperior audit Symantec's Compliance team required successful execution of a 90 day action plan to remedy all findings and a point in time audit proving all remedies were effective.
9) Did Symantec's management or compliance group disclose this qualification to Mozilla?	No. If Certsuperior had not remedied their qualified opinion, Symantec's period of time audit would have reflected that and would have been disclosed to Mozilla.
10) Did Symantec's management or compliance group make its determination of Certsuperior's compliance to Symantec's CP/CPS using Certsuperior's publicly available CP/CPS, which Certsuperior's auditor, Deloitte, noted in [4] that "The policies,	We did not evaluate compliance until a successful point in time audit including assessment of the CPS, was completed.

procedures, and agreements are not available for consultation." and that "The CPS published is illegible"?	
11) If not, what CP/CPS did Symantec use, and how did Symantec ensure it was appropriately audited?	We used the STN CP, the Certsuperior CPS referenced above, and the Deloitte point in time audit letter stating that all findings were remedied. The Deloitte letter is posted to the Bugzilla tracking this discussion.
12) If so, how did you do so, when the auditors themselves were not able to?	Not Applicable.
13) Given Symantec's previous statements regarding "holding ourselves to a 'no compromise' bar" [5], and the numerous issues identified in [4], including an audit finding of "We noted roles of users that are not Trusted Roles with access to validation requests at the web application", a "lack of network segmentation for distinguishing between equipment with access to applications and that which are not part of the validation process", and that Certsuperior's network scans were "not performed with sufficient periodicity and had only ever been executed over the https://www.certsuperior.com website" and "were executed by personnel without technical skill, ethics code, or independence", why does Symantec still have an RA relationship with Certsuperior?	Symantec immediately required a 90-day action plan and point in time audit at 90 days to demonstrate resolution of Deloitte's qualified opinion. Certsuperior complied with the action plan as demonstrated by Deloitte's opinion that the prior findings were proven to be remedied on the date of their point in time audit. Nonetheless, for the broader reasons stated earlier, we have made the decision to terminate our partner RA program.
14) Does Certsuperior pay Symantec to engage as a Registration Authority?	No, RA Partners, like all reseller partners, pay Symantec for sales of Symantec products; there is no fee to engage as an RA.
15) If so, what does Symantec believe should be the reasonable interpretation relative to the continued trustworthiness of Symantec and Symantec's management of the fact that Symantec terminated employees for cause for being involved in misissuance, but has continued to engage in a business relationship with entities who have performed demonstrably worse, but which pay Symantec for that privilege?	Not applicable.
Regarding CrossCert: The audit report indicated in [6] directly states that the audited CP/CPS version of CrossCert is version 3.8.8, available at [7]. This version indicates it was "Published Date: June 29, 2012". This audit was performed by Ernst and Young, Korea. 16) Similar to Q3, is this the correct CPS?	Yes.
17) Similar to Q5, does Symantec believe this CP/CPS, dated in 2012, is consistent with Symantec's CP/CPS, which was updated in response to past misissuances?	The STN CP and the CrossCert CPS state compliance with the CABF BR and such compliance asserts fulsome authentication. We have confirmed that there are deficiencies in the documentation and audit trails for validation performed by CrossCert. We are terminating RA delegation to CrossCert. Further, Symantec's Authentication team is re-validating 100% of certificates issued by CrossCert.
Regarding Registration Authorities 18) Can you confirm that Symantec's response in [2] is correct and comprehensive for all brands directly and indirectly	Yes.

operated by Symantec, including, but not limited to, Verisign, Symantec, Thawte, GeoTrust, and RapidSSL offerings?	
19) Can you confirm that Certsuperior, Certisign, CrossCert, and Certisur are the only Delegated Third Parties utilized by Symantec, across all Symantec operated CAs that are trusted by Mozilla products?	Symantec has three programs where third parties are involved in authentication and or certificate issuance activities: subordination, RA, and processing agent. Subordination includes Google and Apple, who operate CAs that chain to our roots in their premises and submit annual WebTrust audits. RAs include Certsuperior, Certisign, Certisur and CrossCert. This program is being terminated. A processing agent is a delegated third party that uses local language skill to gather organizational identity proof documentation on behalf of their customer. They perform BR 3.2.5 validation of authority, and document the result of that call compliant with BR 5.4.1.2(c) in our audit trail. The information submitted is subject to review by Symantec personnel and Symantec personnel control final decisions on certificate issuance. Xolphin B.V. is a processing agent. As part of terminating the partner RA program, subject to meeting ongoing training and internal audit requirements, we will offer Certsuperior, Certisign and Certisur the ability to transition to processing agents. Given the findings through our investigation we will not be making this option available to CrossCert. Separately, Symantec enables a reseller model. Resellers do not participate in authentication. Symantec's Authentication team performs 100% of the validation and issuance for reseller orders. Subject to meeting separate ongoing legal and compliance requirements, we will continue to make this option available to Certsuperior, Certisign, Certisur, and CrossCert.