Symantec Third Response to Mis-Issuance Questions

Question or Comment	Symantec Response
What criteria is Symantec using to determine if a certificate has a "deficiency" that warrants re-validation? What criteria are Symantec using to judge whether the validation of a particular certificate was deficient and needs redoing? Does this process rely on an assumption that any work logs kept by the RAs are accurate records of work actually done?	As a result of samples we have examined, we have determined that CrossCert record keeping is materially deficient and needs to be revalidated. For each of our other three partners, we will review 100% of archived documentation and the validation methods used. If any certificate documentation has gaps, is incomplete or in any way does not equal the quality standard for our Authentication team, it will be considered deficient. If we determine, on a partner by partner basis, that there are systemic deficiencies in the work historically performed, then we will fully revalidate all certificate details, as we are doing with CrossCert. At this stage we have not identified such deficiencies in the work completed by the other three RA partners. Our standards are based on CABF BR, additional browser policy, guidance from our auditors and our internal knowledge base. Only RA audit trails that match confirming information found at Reliable Data Sources will be considered accurate.
How will Symantec assess whether the domain(s) in a certificate were correctly validated?	All certificates issued using CrossCert RA validation will be revalidated, and if necessary, replaced and revoked. All new certificates issued to these organizations will be issued using Symantec Authentication team validation. For each valid certificate issued by our other three partners, we will use software to access the server(s) named in the CN and SAN(s) to determine whether the certificate installed on those server(s) matches the serial number and issuer of the certificate we are checking. In the case of wildcards, we will attempt substitution of www as the first label of the FQDN. Any certificate containing a CN or SAN(s) that cannot be validated via live access will queue for manual review. For certificates that queue for manual review, Symantec will review the archived domain validation documents for certificates issued by our other three RA partners by revalidating the domains. For any certificate, whether checked manually or by software, where we find that the documentation does not meet our detailed standards for domain validation or used a method that is not supported by the 10 finite methods that were the intent of CABF ballot 169, its successors, and the expected ballots to follow, we will revalidate within these constraints, replace the certificate, and revoke once the customer ceases use of the prior certificate.
Is any of the information gathered by processing agents used for domain validation?	No. Processing agents may only submit links to WHOIS results that are subsequently validated by Symantec's Authentication team manually or ignored and replaced by the results from our

<table>
<tr><td></td><td>WHOIS automation. Processing agents also cannot initiate any automated or semi-automated domain validation methods such as agreed upon changes to web content, DNS tokens, constructed and/or WHOIS contact emails, or domain authorization documents.

Prior domain validations performed by Certisur, Certsuperior and Certisign RAs will be reused for issuance of pending or future certificates only if proven to be performed and documented correctly by Symantec’s Authentication team.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>When you say "Symantec authorized CrossCert to issue certificates from each of the identified CAs", do you mean all five separate certificates listed to the left of this answer in the document? Or do you mean the top list? Or the bottom list? Or something else?</td><td>We mean all five issuing CAs:
https://mozillacacommunity.force.com/001o000000bMjj1
https://mozillacacommunity.force.com/001o000000p4Sdl
https://mozillacacommunity.force.com/001o000000p4SdD
https://mozillacacommunity.force.com/001o000000p4SdK
https://mozillacacommunity.force.com/001o000000p4ScT</td></tr>
<tr><td></td><td></td></tr>
<tr><td>When the revalidation process is complete, will Symantec be reporting on how many certificates were unable to be revalidated?</td><td>Our revalidation will produce (1) confirmation that an existing certificate is properly authorized and the subject information is accurate, (2) replacement of valid certificates with corrected content and documentation followed by revocation or (3) revocation of the certificate without replacement.

We will report a count of certificates for cases (2) and (3).</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Further to your third response, can you provide a list of the certificate fields which CrossCert did or did not have control over, and whether those fields had Symantec-side validation with compliance flagging, and whether those flags could be overridden</td><td>
<table>
<tr><th>Field</th><th>RA Controlled</th><th>(S)creened(2) / Can be (O)verridden</th></tr>
<tr><td>Version</td><td>No(1)</td><td></td></tr>
<tr><td>Serial number</td><td>No, generated by CSPRNG</td><td></td></tr>
<tr><td>Signature Algorithm</td><td>No(1)</td><td></td></tr>
<tr><td>Issuer DN</td><td>No(1)</td><td></td></tr>
<tr><td>notBefore</td><td>Indirectly by date of approval</td><td></td></tr>
<tr><td>notAfter</td><td>Span determined indirectly by end customer choice, can be changed by RA within the max allowed validity</td><td>S</td></tr>
<tr><td>Subject:</td><td></td><td></td></tr>
<tr><td>CN</td><td>No(3)</td><td>S, O</td></tr>
<tr><td>OU</td><td>Yes</td><td>S, O</td></tr>
<tr><td>O</td><td>Yes</td><td>S, O</td></tr>
<tr><td>L</td><td>Yes</td><td>S</td></tr>
<tr><td>ST</td><td>Yes</td><td>S</td></tr>
<tr><td>C</td><td>Yes</td><td></td></tr>
<tr><td>Extensions:</td><td></td><td></td></tr>
<tr><td>SAN</td><td>RA can Add/Delete(3)</td><td>S, O</td></tr>
<tr><td>Basic Constraints</td><td>No(1)</td><td></td></tr>
<tr><td>Key Usage</td><td>No(1)</td><td></td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>EKU</td><td>No(1)</td><td></td></tr><tr><td>CP</td><td>No(1)</td><td></td></tr><tr><td>AKI</td><td>No(1)</td><td></td></tr><tr><td>AIA</td><td>No(1)</td><td></td></tr><tr><td>CRL DP</td><td>No(1)</td><td></td></tr><tr><td>SCT</td><td>No, system generated</td><td></td></tr></table> (1): These attributes and extensions are static values configured in the certificate profile managed by a change controlled process performed by Symantec Trusted Role personnel.(2) Screened refers to scanning for presence of risk keywords. (3) RAs cannot edit CN and SAN in individual certificates. When an RA's enterprise customers request domains to be associated with their organization and enabled for issuance of subsequent certificates, an RA may correct errors in the domain names.
You write: "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". This is great news :-) From what date has this been true? Can you confirm that CAA checking applies to all Symantec-owned brands?	All Symantec brands, channels and platforms enabled CAA checking on various dates ranging from August 20, 2015 to September 15, 2015. We announced support in the STN CPS effective October 1, 2015. This includes certificates issued by all Symantec and reseller-branded issuing CAs within our operations. This excludes two external subordinate CAs chaining to a GeoTrust root and operated by Google and Apple.
Further to your answer about sampling sizes, what (in Symantec's experience) normally defines the sample size an auditor will use when sampling issued certificates during an audit? Is it a fixed number, or defined by the auditor, the issuer, or a dialogue between the two, or some other method?	Sampling size is determined by the auditor using a risk model. It considers automated and manual processes, the CA's historical performance, CA mis-issuance incidents, complexity of the applications involved and coverage of certificate brands with distinct CPS.
http://vtn.certisign.com.br/repositorio/politicas/DPC_da_Cert isign.pdf is dated 2012. BRs section 2 say that the CP and CPS need to be annually updated. Do we understand that this did not happen in the case of Certisign? Same question for CrossCert.	Correct for both RAs, which we refer to as Affiliates in our policy documents. As documented in the STN CP, Affiliates are bound to operate under the requirements of the STN CP. The STN CP was updated 5 times in 2016. The STN CP, Certisign CPS, and CrossCert CPS assert: "CAs within the Symantec Trust Network hierarchy conform to the current version of the CA/Browser Forum (CABF) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at w*ww.cabforum.org*. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document." The audit letter verifies conformity to their CPS. Same applies for CrossCert with that clause.
[…] in Symantec's most recently reply, [1], it seems that again, on the basis of browser questions from a simple cursory examination that such a statement was not consistent with the data - that is, that the full set of issues were not identified by Symantec in their initial investigation, and only upon prompting by Browsers with a specific deadline did Symantec later recognize the scope of the issues. In recognizing the scope, it was clear that the issues did not simply relate to the use of a particular RA or auditor,	Our initial disclosure was released to provide timely information and indicated that our investigation was ongoing. The matters we have reported in subsequent communication result from our own initiative.

but also to the practices of RAs with respect to asserting things were correct when they were not.	
Symantec's also stated that, in response to the past misissuance, it deployed a compliance assessment tool, which functionally serves a role similar to a Validation Specialist. However, such compliance assessment was designed in a way that it could be bypassed or overridden without following appropriate policies.	There are two different relevant system checks in place here: (1) A process that subjects all requests against high risk keywords. This keyword assessment tool is designed to enable manual override because it is non-deterministic and can generate false positives in its advice. The tool will flag high risk terms that are embedded within valid and acceptable terms. For example, www.flatestimate.com will trigger the "test" risk term, alerting the RA to examine the request with the additional scrutiny called for by the BR's definition of a High Risk Certificate Request. (2) A process that subjects all requests, prior to issuance, against a set of technical compliance checks (e.g. SHA1). These cannot be overridden.
Further, as acknowledged in [1], even when Symantec noted that at least one of their RAs had identified specific deficiencies in practice and issuance, Symantec determined it was not appropriate to notify Root Stores or Mozilla of a "problem report".	As stated in the previous disclosure, Symantec followed what it understood to be the appropriate reporting requirements under the Mozilla policy and appropriate based on the results of the external WebTrust audits conducted.
In response to the issues identified in Question 8 of [1], Symantec noted that one of their RAs was deficient in response to its "policies and business practices change in regards to verification procedures for issuing certificates", and allowed 90 days for the RA to remediate this. However, it does not appear Symantec took any corrective action for the period under audit - a year long period - to review any issued certificates during the period of deficiency.	This excerpt does not correctly represent Symantec's response to Question 8 in our second response document. The RA produced a qualified audit and we enforced an action plan and remediation. Symantec was made aware of the need for corrective action at Certsuperior by the qualified audit. Pursuant to the permitted reliance on WebTrust audits in lieu of BR 8.7 self-audit, we did not review issuance nor are any members of the CABF required to review issuance when such audits are performed at least annually.
I highlight this because Mozilla's Policy [7], Item 5, requires such notification to certificates@mozilla.org, but Symantec acknowledges in Question 9 of [1] that it failed to do so.	No event occurred at Certsuperior that is subject to the following Mozilla policy statement: "5. We require that all CAs whose certificates are distributed with our software products notify us when its policies and business practices change in regards to verification procedures for issuing certificates, when the ownership control of the CA's certificate(s) changes, or when ownership control of the CA's operations changes. To notify us of updated policies and business practices, send email to certificates@mozilla.org or submit a bug report into the mozilla.org Bugzilla system, filed against the "CA Certificates" component of the "mozilla.org" product. The request should include the following: - the certificate data identifying the CA certificate(s) that are affected by the change; - copies of (or links to) the updated Certificate Policy or Certification Practice Statement document(s) or equivalent disclosure document(s); and - a summary of the changes that impact the verification procedures for issuing certificates."

Symantec's proposed remediation for these issues appears to be limited to: - Suspend the use of RAs for independent validation of domain control and organizational information	No. It includes: - Termination of the RA program permanently, not suspension - 100% revalidation of approximately 11,600 active Crosscert certificates - 100% automated and manual review of approximately 20,000 active certificates issued by our other three RAs, followed by revalidation as necessary. - Disqualification of two branch offices of E&Y for WebTrust audit opinions - Creation, execution and monthly review of risk flag clearing reports - Retraining of RA personnel to perform a limited processing agent role - Inclusion of all future issuance to customers of these former RAs in our 3% quarterly self-audits such that we specifically achieve the 3% threshold within each former RA's jurisdiction of certificates - Submission of our remediation to our next WebTrust audit
1) Given that the Baseline Requirements require that Symantec accept full liability and responsibility for all actions by Delegated Third Parties, can Symantec please provide what were the specific steps and process Symantec's Compliance Team took in reviewing Registration Authorities prior to the detection of this misissuance? Specific example questions include: a) Did Symantec's compliance team independently assess the WebTrust licensing status of each received audit? b) Did Symantec's compliance team review the CP and/or CPS of each Delegated Third Party to independently assert compliance with the STN CP/CPS?	As posted earlier, in addition to relying on the results of independent WebTrust audits, for which the answers to (a) and (b) are "yes", we also: (i) put in place systematic controls that applied to all certificates, regardless of source, to block and require manual review of potential cases of mis-issuance based on our own experience, (ii) continued our practice of requiring annual exams on current practices with RAs that made no distinction for test certificates, (iii) instituted technical checks both prior and subsequent to issuance that applied to all certificates, regardless of source, to block known areas for potential violation like SHA1, (iv) implemented CAA that applied to all certificates, regardless of source, to enable customers to define for themselves the CAs that they wanted to trust, and (v) implemented CT logging for all certificates, regardless of source, and developed a CT monitor to enable customers to assess for themselves whether certificates issued for their domains were legitimate.
2) Given that Symantec has noted that RAs bore the capability to override the results of the compliance tool, can Symantec please provide details about every certificate Symantec has issued which has had the compliance check overridden?	Our compliance checks include BR mandates that cannot be overridden as well as high risk terms contained in the fields we explained are screened above. Term screening can produce false positives. Flag clearing does not permit a technically enforceable BR to be violated, it permits an RA to assert that the high risk word is present but validation proves the data in the field to be accurate and verifiable. We can provide CT log links to all 30,000+ certificates. We may be willing to provide flagged orders on a limited basis, subject to NDA, but given the volume of certificates in question we will not publish this publicly as it could enable a third party to reverse engineer the flagging triggers we check for.
3) Symantec noted in [5] that "Each certificate request is screened for BR compliance failure. Failures are flagged, preventing RA issuance until the flag is cleared." Can	Confirmed. Certificates are not issued unless they contain zero technically enforceable BR violations, such as subject locality and

Symantec please confirm that "RA issuance" refers to the act of Symantec signing a TBSCertificate and producing a signed certificate, as opposed to any other interpretation, such as Symantec signed the certificate, but did not provide it to the RA until the flag was cleared?	state presence, and all risk word flags are cleared as false positive matches. Further, note that the only flags that can be overridden/cleared are those raised for high risk words.
4) Was the problematic audit, highlighted in Questions 10 and 11 of [1], CertSuperior's first audit as a Symantec RA? Stated differently, did Symantec engage in any business relationship with CertSuperior prior to the production of [8]?	No. Yes.
5) Symantec's initial response to Mozilla, in [6], indicated that Symantec will be conducting "a review of our delegated RA controls and why we did not detect this problematic behavior before it was reported to us". What is the timeline for when this review will be completed and published?	Based on the review that we have conducted to-date, the findings from which we already published, and the decision to terminate the program and check the validation on all active certificates, we are suspending any further investigation.
6) Please provide the specific dates that Symantec engaged in a Delegated Third Party relationship with each of the RAs, so that the community can independently evaluate the 'scope of the issues' with respect to what certificates may be affected by the issues Symantec has disclosed.	Each of these relationships pre-dated the acquisition by Symantec of the VeriSign Trust Services business in 2010.
7) Are there any elements in the above comparison between the past and present misissuance that Symantec believes are factually incorrect or unsubstantiated that Symantec would like to address or correct?	There are several elements in your comparison that are factually incorrect. https://www.symantec.com/page.jsp?id=test-certs-update# details three root causes and associated remediation of the previously reported mis-issuance. https://www.symantec.com/about/legal/repository.jsp links to the unqualified point in time audit reports following the remediation of the previously reported issues. To be clear, the scope of the 2015 incident involved more procedures that generated mis-issued test certificates than a single testing tool.
Questions dated February 17, 2017: 1) Was Symantec's compliance team involved in the review of Certisign's audit? 2) Does Symantec agree with the conclusion that, on the basis of this evidence, Symantec failed to uphold the Baseline Requirements, independent of any action by a Delegated Third Party?	Yes, we reviewed the calendar year 2015 audit when initially received in January, 2016 and noted a date error that EY Brazil was delinquent in correcting. No, EY Brazil was licensed for the CY 2015 audit period: https://web.archive.org/web/20140805013053/http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx https://web.archive.org/web/20160314032243/http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx