Symantec Responses to Mis-Issuance Questions

Reference [1]: https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&id=INFO4154

Question	Symantec Response
1) In response to the previous incident, Symantec indicated they hold a "no compromise" bar for such breaches in the post titled "A tough day as leaders".	
a) Do you believe that the steps to "reduce privileges" represent a consistent application of that standard?	We believe the steps we have taken and are taking appropriately respond to the incident and we will continue to evaluate whether other steps are necessary as our investigation continues. See also [1] Immediate Response #1.
b) If not, what additional steps are you taking, consistent with your "no compromise" standard?	We disabled CrossCert issuance privileges. We revoked 31 certificates within 24 hours of notice. We have taken over issuance internally. We disabled access to enterprise accounts provisioned by CrossCert. See also [1] Immediate Response #1-4.
2) In response to the previous incident, Symantec indicated that the use of any privileged test tool would require senior leader justification from both QA and Production Operations teams and approvals from the heads of Engineering and Policy Compliance.	
a) Did Symantec mean that this was limited to validations performed by Symantec, and not that of Registration Authorities fulfilling the duties pursuant to Section 1.3.2 of the Baseline Requirements?	The privileged test tools referred to in our previous disclosure were only accessible to internal Symantec personnel, not to RA partners. [1] Root Cause #6.
b) At the time Symantec made this statement, did Symantec have any Registration Authorities fulfilling the duties pursuant to Section 1.3.2 of the Baseline Requirements?	Yes, but no RA partners had access to these privileged test tools.
c) If such a statement was meant to be limited to Symantec, and not that of Registration Authorities, why did Symantec not feel it was appropriate to highlight that it did not extend to activities performed by Registration Authorities?	RA Partners do not have access to these tools. [1] Root Cause #6.
d) If such a statement was not meant to be limited to Symantec, was such a justification provided, and approvals granted, for the tool that allowed such Registration Authorities to issue these certificates?	Not Applicable.
3) In response to the previous incident, Symantec indicated a comprehensive review of issuance privileges was conducted to ensure only authorized personnel have the ability to issue certificates, and that a quarterly access review would be conducted to ensure this.	
a) Did such comprehensive review include that of Registration Authorities?	Yes.
b) If not, why did Symantec not disclose that Registration Authorities were excluded?	Not Applicable.
c) Is Symantec currently performing access reviews of Registration Authorities?	Yes, they are included as part of our audited monthly access review process.
d) If so, when does Symantec expect this to be completed?	Not Applicable.
4) In response to the previous incident, Symantec indicated it updated its internal policies and procedures for test certificates as used for commercial certificates. Further, it indicated that QA engineers and authentication personnel were trained on updated practices for test certificates.	
a) Did Symantec include Registration Authorities in the scope of that training?	We did not train partners on an issue that pertained to a tool they could not access.
b) If not, why did Symantec not disclose that Registration Authorities were excluded?	The training referred to in our previous disclosure was delivered to Symantec QA and Authentication teams guiding them to eliminate non-standard testing procedures for obtaining public certificates. Our delegated RA partners do not perform a QA function. Our delegated RA partners are trained to always issue only fully validated certificates. At no point

	were RA partners authorized to perform less vetting on certificates for their own internal use.
c) If so, why did Symantec's corrective actions for the previous mis-issuance fail to prevent this continued mis-issuance?	Not Applicable.
5) You have indicated that you have at least one WebTrust audited partner capable of causing issuance using Symantec-operated CAs.	
a) Please provide a link to the audit results for each of these WebTrust audited partners.	CrossCert (Korea Electronic Certificate Authority): https://cert.webtrust.org/SealFile?seal=2167&file=pdf https://cert.webtrust.org/SealFile?seal=2168&file=pdf Certisign Certificatadora Digital: See attachments posted at https://bugzilla.mozilla.org/show_bug.cgi?id=1334377 Certsuperior S. de R. L. de C.V.: See attachments posted at https://bugzilla.mozilla.org/show_bug.cgi?id=1334377 Certisur S.A..: https://cert.webtrust.org/SealFile?seal=2067&file=pdf
b) Have you suspended the capabilities of these partners until Symantec completes its investigation?	Only CrossCert.
c) If not, why not, and when do you expect to do so?	Our ongoing investigation includes activities of our other delegated RAs. At this time we do not have evidence that warrants suspension of privileges granted to any other RA besides CrossCert.
6) Does Symantec allow is Registration Authorities to deviate from the policies and standards set forth by its CP, CPS, and internal policies and controls?	
a) If not, why did Symantec fail to detect that its Registration Authorities were deviating from its policies for this long?	RAs are required to follow the same policies as set forth in Symantec's CP and CPS documents. Internal procedures at an RA are subject to their WebTrust audits to ensure conformity with the associated policies. - Our investigation is proceeding, but to our knowledge only CrossCert is involved. - We evaluate independent WebTrust audit reports for material findings. In the case of CrossCert, their last audit report was unqualified by E&Y South Korea and the problem certs identified in category A, B, D, E, and F were all issued subsequent to that last audit. Category C concluded prior to that last audit's review period. - Based on these findings, we intend to implement additional direct monitoring and audit of RA activity to supplement the independent WebTrust reports, with the objective of quickly detecting and blocking similar cases in the future.
b) If so, where does Symantec disclose this deviation within its CP and/or CPS?	Not Applicable.
7) When do you expect to provide the next update as to the ongoing investigation? If it is not within the next three days, why?	Published on Jan 26, 2017.
It's not clear what the problem is with the issuance in category F. I don't see any mention of "dev119money.com" in Andrew's initial report. Can you explain (and provide a crt.sh link)?	This certificate contains "test" in four DN attributes including Organization. It is isolated from Category D because the common name dev119money.com is not a registered domain, 119money.com is. The omitted dot separator after "dev" repeats in the SAN extension. This is a domain validation error. https://crt.sh/?q=48539119

Root Cause, bullet 2 refers to "certificates issued between July 2016 and January 2017"; is it correct that this corresponds to categories A (one of four certificates), B, D, E and F?	Correct.
What processes, other than requiring and inspecting a WebTrust report, does Symantec have in place to ensure that its RAs behave in accordance with the CP and CPS of the Symantec-owned roots under which they are issuing? (Perhaps this will be covered in the report you will issue after the "additional follow-up" steps are completed?)	Software: 1. Each certificate request is screened for BR compliance failure. Failures are flagged, preventing RA issuance until the flag is cleared. 2. Each request is screened, for example, using a list of risk words such as “test”, strings used in scam domains, and high-profile brands. String matches are flagged for risk. Risk flags require manual override by RA personnel who have passed their exams and who are granted validation and flag clearing privileges by Symantec administrators and can refer to our knowledge base for flag reason explanations to understand the purpose and severity of the flag. See [1] Root Cause 2-3. 3. Each request is screened for BR compliance again when the RA approves the request and before it is issued. 4. Daily, we rescan all certificates issued on the prior day. Training 1. Topics include BR changes, CPS changes, process changes as a result of industry incidents regardless of the CA involved, and a review of Symantec’s procedures that extend the Baseline Requirements. 2. Exams are modified and retaken annually as criteria to renew individual access certificates or after significant internal or external process change. Documentation 1. Symantec operates an internal knowledge base accessible by RA partners that contains detailed step by step procedures for performing each of the tasks required to validate the identity asserted in a certificate request. 2. The KB reinforces acceptable and unacceptable sources of validation information and processes using a subset of the information in the BRs. 3. The KB explains request flagging, flag reasons, and flag clear procedures. Audit 1. We evaluate the RA’s independent WebTrust audit reports for material findings pursuant to BR 8.4 regarding WebTrust audited Delegated Third Parties.
Do such processes include regular, occasional or any review of the audit logs which show the overriding of compliance failure flags?	No. We intend to implement flag clear reporting, review the reports for unusual patterns, and investigate when appropriate. See also [1] Additional Follow-up #4.
Were the web identities (DNS names etc.) in the category C, D, E and F certificates properly vetted as per the CP/CPS etc., the certificates simply replaced the vetted organization name with "test" in the X.500 distinguished name? Or were some of those issued for insufficiently (or actually incorrect) web identities?	CrossCert has stated that vetting was performed properly for identity information in its certificates. We are currently validating that claim. Symantec has requested all proof of right documentation from CrossCert for the 127 certificates. We are analyzing all certificates issued by CrossCert and will request documentation for a random sample of certificates. If our

	analysis finds suspicious certificates, we will request documentation. Our auditors, KPMG, completed a scan of CrossCert certificates to detect potential mis-issuance and presented 12 suspicious certificates. We treated this as a certificate problem report under the BRs and began an investigation. We released a disclosure that described what we found that led to revocations.