1	Q1) Symantec's audit for 2014-2015: https://www.symantec.com/content/en/us/about/media/repository/GeoTrust-WTBR-2015.pdf says on page 11: "We noted that audit reports were not obtained during the examination period for 2 of 5 external partner subordinate CAs signed by the GeoTrust Global CA and managed by contracted third parties as part of the GeoRoot service). In addition, the report obtained for 1 of 5 external partner subordinate CAs was not in accordance with permitted audit schemes. Furthermore, in lieu of third party audits completed by delegated third parties, no out-of-band mechanisms were used to confirm the authenticity of the certificate requests, or the information supporting the certificate and internal reviews were not performed by Symantec to determine third party compliance with baseline requirements. For the 2 external partners where reports were not obtained during the examination period, one external partner's subordinate CA has since expired and Symantec subsequently received an audit report for the other. For the other external partner, Symantec reviewed the report obtained and requested that their next report be in accordance with permitted audit schemes." A) Can you please identify all of the companies referenced here, by putting names to each reference? B) When the second paragraph, beginning "Furthermore", refers to "delegated third parties", does it mean the same five subordinate CAs as the first paragraph, or does it refer to the RA program that you recently shut down? C) If it refers to the same subordinate CAs, can you explain how the RA audits for CrossCert, Certisign, Certsuperior, and Certisur featured in the 2014-2015 auditing process? Where they examined by KPMG?	A. See Symantec response for Issue V [https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/Ga1bfOiJr70]. B. This was a continuation of the first paragraph, referring to Intel, Aetna, Unicredit, Google, & Apple. See issue V. C. For both the RA program and the GeoRoot program clarified in Issue V, KPMG focused on our receipt of audit reports from these third parties, continuity from previous periods, the audit opinions, and in the cases where there were issues identified, Symantec's plan of action to remediate. In this case, Symantec and KPMG failed to note that we were missing some of the required audits.

2	Q2) Please give the names of all companies who have been in your RA program recently enough that there still exist unexpired certificates which were issued by them, and their start and end dates in the program. Although we have had some of this information before, for completeness please provide links to all audits for each company.	The start dates of our SSL/TLS RA partnerships are all prior to 2010 when Symantec acquired the Trust Services business from VeriSign and prior to the BRs going into effect. During the period of 2011-2014 we significantly reduced the number of these RA partners that could issue SSL/TLS certificates and restricted all but CrossCert, Certisur, Certisign, and CertSuperior to perform validation for SSL/TLS certificates. We imposed technical measures to prevent all SSL/TLS validation and issuance capabilities by all RA's except for these four partners, In 2017 we took the additional step of removing the ability of these remaining four partners to issue SSL/TLS certificates which represented a complete wind-down of the SSL/TLS RA program. See Item W for more details of the RA program: [https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/Ga1bfOiJr70]. The following affiliates operated as an RA for Symantec SSL/TLS certificates, conducting authentication and issuance activities. This list does not include additional partners who had been terminated prior to the acquisition of the Trust Services business from VeriSign, Inc. in August 2010 as there are no unexpired certificates issued by these former partners. The end date referenced below is the date of the last SSL/TLS authentication event by the affiliate within a customer's Enterprise RA account. As of April 19, 2017 all certificates counted below were certificates issued out of domain-constrained Enterprise RA accounts originally authenticated by the affiliate. Numbers represent still active certificates issued using the authentication work by the affiliate. That issuance, subsequent to the affiliate SSL/TLS termination, has been possible leveraging the 39-month data validity rule for OV/DV certificates. <u>End date in 2017</u> Audits at https://bugzilla.mozilla.org/show_bug.cgi?id=1334377 **CrossCert** End date: January 19, 2017 Active certificates: 10,603

CertSuperior
End date: April 4, 2017
Active certificates: 4,430

CertiSign
End date: April 11, 2017
Active certificates: 13,521

CertiSur
End date: April 14, 2017
Active certificates: 2,935

End date between 2011 - 2014
These RA for SSL/TLS relationships were wound down as the BR's went into effect. We do not have audits for them.

Note, while no longer authorized as affiliate RAs for SSL/TLS, many of these partners continue to offer SSL/TLS for sale as Symantec resellers.

Adacom S.A.
End date: November 15, 2012
Active certificates: 2

Comsign, Ltd
End date: February 14, 2013
Active certificates: 15

e-Sign S.A.
End date: March 4, 2013
Active certificates: 16

iTrusChina
End date: January 11, 2013
Active certificates: 52

NamITech
End date: November 7, 2012
Active certificates: 167

Telefonica S.A.
End date: February 5, 2014
Active certificates: 88
* Note, in our response on issue T indicated that the RA program for SSL/TLS was wound down in 2013. That should have stated 2014 to reflect Telefonica.

MSC Trustgate.com Sdn Bhd
End date: February 8, 2013
No active certificates

mySecureSign, Inc.
End date: August 22, 2011
No active certificates

Safescrypt Ltd
End date: June 25, 2012
No active certificates

NIFTeTrust
End date: September 6, 2013
No active certificates

With the exception of Telefonica, all previous org/domain validation data is now outside of the 39 month rule. In the case of Telefonica, we are disabling use of previously validated org/domain information otherwise still valid under the 39 month rule. After this update Symantec will solely authenticate new certificate issuance for all of these customer accounts originally authenticated by these partners.

There were also questions regarding issuance controls on RA certificates. In our infrastructure there are a few different cases:

For Publicly Trusted Class 3 CAs: These include CAs that can be used for multiple purposes, including server authentication, as defined in our CPS.

1. With the exception of the GeoRoot CAs, all Class 3 CAs and sub-CAs are operated out of Symantec controlled infrastructure.

		2. With the wind-down of the SSL/TLS RA program, all authentication and issuance of certificates chaining to Class 3 CAs is done by Symantec; Google and Apple in the case of the GeoRoot sub-CAs; and customers of the Non-Federal SSP program (in this case used to issue certificates for Microsoft Windows domain controllers and IPSec endpoints). 3. The GeoRoot sub-CAs operated by Google and Apple are fully controlled by those organizations and audited. For Publicly Trusted Class 1 & 2 CAs: These include CAs that can be used for multiple purposes, excluding server authentication, as defined in our CPS. 1. Class 1 & 2 sub-CAs are operated out of Symantec's infrastructure, and separately out of (non-TLS) RA infrastructure using software provided by Symantec. 2. Symantec limits issuance of public TLS server authentication certificates chaining to Class 1 & 2 CAs through both its own software configuration and (non-TLS) RA software configuration. 3. Symantec authorizes (non-TLS) RAs to have access to publicly trusted sub-CAs dedicated exclusively to their use, compartmentalizing each affiliate. These are only signed by Class 1 & 2 Symantec sub-CAs that chain up to Class 1 & 2 roots. 4. Browser vendors control the trust bits assigned to roots. We have verified in the cases of Microsoft and Mozilla that those controls do not grant server authentication trust for our public Class 1 and Class 2 roots or any sub-CAs operated under them, in accordance with our CPS. In addition to the actions we have already taken, we are currently conducting a thorough review of the non-TLS RA program.
3	Q3) Please give the names of all companies who have been in your GeoRoot program recently enough that there still exist unexpired certificates which were issued by them, and their start and end dates in the program. Please provide links to all audits for each company.	Apple and Google are the only remaining active GeoRoot program partners. Audit information for both are accessible via the Mozilla Common CA Database. Intel, Aetna, and Unicredit CAs have all expired or been revoked.

4	Q4) Are there any other programs Symantec runs or has run in the past five years, other than the recently-terminated RA program and the GeoRoot program, which puts either the power of domain ownership validation or the power of certificate issuance in the hands of an organization other than Symantec or its Affiliates? If so, please give details of the program, and lists of companies, dates and any applicable audits as outlined above.	There are no other such programs related to SSL/TLS issuance nor third parties in the RA and GeoRoot programs that have not been previously disclosed. For clarity, NTT DoCoMo is covered under the scope of Symantec's WTCA & WTBR audits, as stated in issue V. As stated in issue X, Symantec operates an RA program for non-SSL/TLS certificates.
5	Q5) You have recently released your 2016 audits, split into two parts at June 16th (6.5 months into the 12-month period). The audits for the first six months contain almost all of the qualifications that the 2015 audits have. Please can you give exact or approximate dates for "start of issue", "discovery of issue" and "problem fixed/ceased" for each of the following issues which led to a qualification: A) Test certificates issued for domains Symantec did not own or control B) Failure to maintain physical security records for 7 years C) Unauthorized employees with access to certificate issuance capability D) Failure to review application and system logs E) Background checks not renewed for trusted personnel after 5 years	A1. For test certificates to registered domains: Start of issue: Jan 2, 2009 Discovery of issue: Sep 16, 2015 [Externally reported] Problem ceased (last issuance): Sep 15, 2015 Problem fixed: (last revocation of all identified related certs): Mar 16, 2016 While inappropriate use of registered domains for testing stopped during the course of our 2014-2015 audits, we did not complete the ID and revocation of all certificates until Mar 2016, and so the finding remained in our first-half Dec 1, 2015-Jun 15, 2016 audits. A2. For test certificates to un-registered domains: Start of issue: Apr 14, 2009 Discovery of issue: Approximately Oct 2015 during test certificate investigation Problem ceased (last issuance): Oct 6, 2015 Discovery of additional instance involving approved domains in a test account resulting in 6 additional issued certificates: Approximately Mar 2016 Problem ceased (last issuance): Mar 7, 2016 Problem fixed: (last revocation of all identified related certs): Mar 16, 2016 B. Failure to maintain physical security records for 7 years started in September 2015. It was identified and immediately corrected in January 2016. C. The test tool referred to in our 2015 test certificate disclosures was created in 2006. We identified the issue with use of that tool outside of its intended purpose on September 16, 2015, and it was remediated in October 2015. Over the following months, we conducted a

		comprehensive review of access privileges across systems and put in place enhanced monitoring. During the course of that work, we addressed any cases where we determined that the principle of least privilege was not fully enforced. That work was completed in June 2016. D. Failure to review application and system logs started in Sep 2015. It was identified and immediately resolved in Jan 2016. E. The failure to refresh background checks every 5 years began in Oct 2015. We identified this issue in Feb 2016 and fully remediated it by June 2016. The approximately 4-month remediation involved working within local government regulations and HR guidelines in each of our locations, and reorganizing the internal teams responsible for this work.
6	Q6) The management assertions in the audits for neither the first-half nor the second-half of 2016 contain any qualification related to the audit status of either your GeoRoot or RA program partners. Does this indicate that Symantec felt that all partners in these programs were in good standing audit-wise during the period from December 1st 2015 to November 31st 2016?	No, as we shared in our response to issue V, we acknowledge there were deficiencies in audits for both the GeoRoot and RA programs. The plan for the GeoRoot deficiencies was communicated in the cover letter accompanying our Point in Time audit (see issue V) and for the RA program, in the cover letter to browsers with our 2015-2016 audits: https://www.symantec.com/about/legal/repository.jsp?tab=Tab3
7	Q7) In your comments at the time on what is now labelled Issue D, the misissuance of test certificates, you wrote: "First, we continued to issue internal test certificates to unregistered domains after the April 2014 change in the Baseline Requirements that removed authorization to do so." By "the April 2014 change", do you mean by ballot 112? If so, can you explain how you see this ballot as affecting the correctness or otherwise of issuing certificate for unregistered domains?	Yes. That change struck the parenthetical "(which may or may not include an Unregistered Domain Name)." The term UDN is not referenced in any other part of the BR. For clarity, our disclosure of mis-issued test certificates was based on the following: 1. Any EV test certificates ever issued to unregistered domains, and 2. Any OV/DV test certificates issued after April 3, 2014 (the effective date of BR version 1.1.7, incorporating ballot 112).
8	Q8) The accountant's letters for the 2015-2016 audits are dated February 28th 2017. The audits were supplied to Mozilla, and published, on the 1st of April 2017. Why the delay?	Proofreading of the reports, corrections, and clarifications took an additional four weeks. KPMG provided an explanation of the delay in their explanatory letter which has been provided, and which centered on the large scope and resulting sheer volume of audits.

9	Q9) Can you please tell us which audit covers the following two intermediate CAs, which are subordinates of or cross-certified by VeriSign Universal Root Certification Authority? VeriSign Class 3 SSP Intermediate CA - G2 (https://crt.sh/?Identity=%25&iCAID=1384&exclude=expired) Symantec Class 3 SSP Intermediate CA - G3 (https://crt.sh/?Identity=%25&iCAID=12352&exclude=expired) The following period-of-time audit is the most recent one which covers the VeriSign Universal Root Certification Authority: https://www.symantec.com/content/en/us/about/media/repository/18_Symantec_STN_WTCA_period_end_11-30-2016.pdf However, these certificates are not on the accompanying list of intermediates. Is it correct that these intermediates are unconstrained and fully capable of issuing server authentication (SSL/TLS) certificates which are trusted by Mozilla browsers?	These Intermediate CAs are sub-CAs under the Verisign Universal Root CA. They are covered under Symantec's Non-Fed SSP audits, and the latest unqualified audits that we just received are being published. The customer-specific CAs (the subordinate ICAs) signed by these sub-CAs are path length constrained and operate fully within Symantec's infrastructure. Under the Non-Federal SSP program, they are used to issue certificates for Microsoft Windows domain controllers and IPSec endpoints. End entity certificates issued under this program are designed only to contain Federal PKI policy OIDs and to exclude any CA/B Forum required policy OIDs.
10	> Separately, Symantec operates two subordinate CAs solely for NTT > DoCoMo in an enterprise PKI application. These subordinate CAs had > been considered part of the "GeoRoot" program as well, and we had > therefore excluded them (similar to the above externally operated > ones) from the list of Symantec CAs in our audits. If they were excluded from the Symantec audit, and were not one of the five GeoRoot partners who had their own audits, did these subordinate CAs fall under any audit at all in this period?	All authentication performed for the NTT CA's has been completed by Symantec personnel. The authentication applications used have historically been fully within the scope of our WTCA/WTBR audits. The infrastructure on which this specific enterprise PKI application and those CAs operate was not covered under audit until these CAs were added to the 2015-2016 audits.
11	> Symantec provided the letter quoted below to Google, Mozilla, > Microsoft, and Apple when we shared the Point in Time Audits on > September 6, 2016 to specifically address the GeoRoot audit status and > remediation plan. Without seeming to doubt your word, can you tell me how you supplied such a letter? Was it to certificates@mozilla.org or directly to Kathleen? A	**Sent:** Tuesday, September 06, 2016 12:40 PM **To:** kwilson@mozilla.com **Subject:** Symantec Website Security Point in Time Audit

	quick search can't find it in my email archive, so a recipient, Subject and Date for the communication would be most appreciated.	
12	> All of Certisign's audits are both WebTrust for CAs and SSL Baseline > and were unqualified. The Certisign audit provided was this one: [link] It does say that Certisign complied with the Network Security Guidelines but doesn't mention the BRs and, somewhat confusingly, also says: "This report does not include any representation as to the quality of CERTISIGN - CA's services beyond those covered by the Trust Service Principles and Criteria for Certification Authorities..." which suggests this audit is only a WebTrust for CAs audit, not a BR audit. Are there audit documents missing which show that they were BR-audited? Can you clarify?	The Certisign 2012 audit meets WebTrust for CAs criteria because the SSL Baseline audit was not required until periods beginning January 1, 2013. For Certisign's 2013 audit, please refer to the end of the first paragraph on the second page for the following clause: "based on the AICPA/CICA Trust Services Criteria for Certification Authorities and SSL Baseline Requirements Audit Criteria." For Certisign's 2014 audit, please refer to the end of the first paragraph on the second page for the following clause: "based on the AICPA Trust Service Principles and Criteria for Certification Authorities, Version 2.0 and SSL Baseline Requirements Audit Criteria, Version 1.1." For Certisign's 2015 audit, please refer to the end of the first new paragraph on the second page for the following clause: "based on the AICPA Trust Service Principles and Criteria for Certification Authorities, Version 2.0 and SSL Baseline Requirements Audit Criteria, Version 1.1." Certisign's 2016 audits are past due. We have notified Certisign.
13	> Certsuperior's audits state that their scope was WebTrust for SSL > Baseline but do not state WebTrust for CAs. Prior to 2016, > Certsuperior provided WebTrust SSL Baseline audits from an unlicensed > auditor. Symantec's compliance organization identified the issue in > 2016. For 2016, Certsuperior provided a qualified audit by Deloitte, a > WebTrust licensed auditor in Mexico. Certsuperior's audit led to > immediate sanction to solve the issues detected within 90 days and to > provide a Point in Time audit. They provided such audit and it was > unqualified. Further, Deloitte is required to examine certificate > issuance as a normal part of the WebTrust program and they did not > cite any problems with Certsuperior's validation work in either audit. > Accordingly, we believe certificate issuance was inspected. Are you saying that none of the deficiencies identified at Certsuperior, in Symantec's view, had a material effect on the quality of certificate issuance?	The CPS legibility did not factor into our interpretation of the audit – just the audit findings themselves. Our concerns about the findings in the audit led to the 90 day correction period and required Point in Time audit. We are almost complete reviewing Certsuperior's certificates. Of Certsuperior's 4,430 active certificates, we have completed review of 4,316 and found the following: - 4088: No Issues - 228: Errors Error reasons include spelling mistakes in information in the organization name, imprecise values in locality (related to the name change of Distrito Federal to Ciudad de Mexico), and any cases where

	Given that Deloitte pointed out that the CPS was illegible and there was a "lack of implemented and documented control for requested validations sent by authorized personnel", on what grounds do you state that "Deloitte ... did not cite any problems with Certsuperior's validation work"? If they can't read the CPS, how can they tell if Certsuperior is following it?	we did not receive sufficient documentation to substantiate subject information. These certificates were revoked within 24 hours.
14	> Certisur's audits were WebTrust for CAs only. Symantec's compliance > organization identified the issue and has requested that Certisur's > next audit for calendar year 2016 explicitly include the criteria in > both WebTrust for CAs and WebTrust Baseline. All audits received were > unqualified and performed by a licensed WebTrust auditor. How long has it been the case that they did not have a BR audit?	According to our records Certisur has only provided WTCA audits and no WebTrust SSL Baseline audits since such audits became required.
15	> CrossCert's audits were WebTrust for CAs only through 2015. Same question. Does Symantec agree that these RAs should have had a Baseline audit for all periods when they were operating?	Yes, we agree and we have requested that both be provided for subsequent audits.
16	On 10/04/17 17:20, Ryan Sleevi wrote: > 1) You stated that this partner program applies to non-TLS certificates. > The audit for both STN and for the RAs fails to make this distinction. > For example, audits are listed related to the issuance of of TLS certificates. The audits linked to from the wiki page relating to E-Sign and MSC TrustGate don't seem to have any mention of TLS certificates. Can you explain which audits you are referring to above that do mention them?	Both E-Sign and MSC TrustGate have had a long relationship with Symantec dating prior to the effective date of the Baseline Requirements. Both partners stopped operating as RAs for SSL/TLS certificates but continue to operate as RAs for Class 1 and Class 2 certificates. The audits do not typically call out any specific usage of the CAs under the audit. This is a good clarification point that we will implement in third party audits in the future.
17	> 1) On the basis of the controls Symantec described, at no point was > any mention made of Symantec performing sampling audits to ensure > their RA partners complied with either the RA partner's CP/CPS or Symantec's CP/CPS. > a) Is it fair to conclude that no such examination if done?	We are an active participant in the CABF, and take the Baseline Requirements and other policy requirements very seriously.

	In various rounds of questioning at the time we were focusing purely on this incident, I asked Symantec what processes they had in place for checking that the RAs were doing what they should. Their answer was "WebTrust audits". So I believe they have already said that no such examination was done. I'm sure they'd be happy to clarify, though. Most of your other questions are fairly stated (if perhaps rather broad in scope - are you expecting a total dump of all their internal procedure documents?). But particularly: > d) Is it fair to conclude that Symantec's belief is that it does not > have to follow the Baseline Requirements that it disagrees with?	
18	Issue B 2) You've noted that you did not disclose it due to "contractual obligations to protect the customer's privacy", which "remains in force". a) If a contractual obligation is in conflict with the Baseline Requirements, do you have a process defined to resolve that conflict? If so, please fully describe it. b) If a contractual obligation is in conflict with other Root Program requirements, do you have a process defined to resolve that conflict? If so, please fully describe it?	We have hundreds of thousands of customers with whom we have agreements in which we commit to preserving their privacy. We do not believe that preserving customer privacy is in conflict with the BRs.
19	Issue N 1) What steps, specifically, has Symantec taken to ensure such clarity is provided in the future? 2) What steps, specifically, has Symantec taken to ensure appropriate review prior to the execution of such processes? These questions apply to any process involving CA key material, including, but not limited to, certificate signing ceremonies or the bringing online of an offline root. ---	We updated and clarified the written procedures for this new process.
20	Issue P	This was a customer operated CA and we did not have access to the private key.

	1) Why was Symantec unable to operate the CRL service for Unicredit?	
21	Hi Steve, Some follow-up questions: 1) Symantec stated "This information was in their management assertions, and repeated in the audit findings. So the poor audit situation was ongoing and known." a) Symantec did not meaningfully provide any explanation, now, or in the past, as to why it took multiple audit periods to resolve these issues. In order to establish for Relying Parties that Symantec is trustworthy and competent, please supply additional details as to why it took so long.	We agree that getting audits for Aetna and Unicredit took too long. After many discussions, requests, and delays, they finally produced the reports that they did. This experience informed our decision to transition them to alternative solutions.
22	Issue R – Alex Gaynor Hi Steve, Tiny nit-picky follow up question. You said: "it's technically not feasible. This is because Symantec does not have access to our customers' TLS server private keys.". X.509 certificates can of course be used for things besides TLS, when you say "TLS server private keys", is that meant to indicate a contrast with other customer private keys, which Symantec does have access to? Or is it accurate to say that "Symantec does not have access to our customers' private keys"? Thanks, Alex	To further clarify, we do not have access to private keys associated with TLS certificates. For non-TLS certs, we do operate a code/document signing service, where we operate/manage signing keys on behalf of customers. Additionally, for S/MIME certificates, there is an optional key escrow service in which case we do have access to S/MIME private keys for customers who choose to use that service.
23	Issue X James Burton On Monday, April 10, 2017 at 4:00:21 PM UTC+1, Steve Medin wrote: > Issue X: Incomplete RA Program Remediation (February - March 2017) > > The only Symantec RAs capable of authorizing and issuing publicly trusted SSL/TLS certificates are: CrossCert, Certisign, Certsuperior and Certisur. Symantec continues to maintain a partner program for non-TLS certificates. E-Sign SA and MSC Trustgate are amongst these partners.	Yes, this is the complete list – when we refer to “Symantec” here, we are including all Symantec Corporation owned and operated CAs that chain up to public Symantec, GeoTrust, & Thawte branded roots and operating under the respective CP/CPS’s.

	Are you sure? As this seems far too low. Did GeoTrust and Thwate have RAs capable issuing publicly trusted SSL/TLS certificates? James	
24	>Within a few days of discovering these issues they shut down their >entire RA program. That seems pretty swift and comprehensive to me. The >fact that they didn't discover these issues for years is clearly a >problem, but it's not the same problem. I don't believe that's a fair characterization--looking at https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&id=INFO4154 it was more like "After approximately 3 weeks (Jan 19-Feb 12) they *decided* to shut down their RA program." ("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.") Their latest update (approximately 3 months from the initial report) is that "Symantec announced the decision to wind down the RA program for publicly trusted SSL/TLS." While Symantec re-validating each issued cert from their RA's is good, and it appears CrossCert is fully terminated, they clearly have not "shut down their entire RA program."	To clarify, Symantec has shut down the SSL/TLS RA program across each of CrossCert, CertSuperior, Certisign, and Certisur. In all cases, we are revoking certificates that present issues within 24 hours in accordance with BR section 4.9.1.1. 1. CrossCert: any still active test certificates identified in the initial investigation were revoked within 24 hours. Following that, our decision to revalidate 100% of Crosscert–issued certificates was driven by CrossCert's incomplete logging of telephone validation call activity under section 5.4.1.2.c. Of 10,603 active certificates, we have completed review of 80% and found the following: - 8259: No Issues - 200: Errors 2. Certsuperior: of 4,430 active certificates, we have completed review of 97% and found the following: - 4088: No Issues - 228: Errors 3. Certisign: of 13,521 active certificates, we have completed review of 64% and found the following: - 8651: No Issues - 34: Errors 4. Certisur: of 2,935 active certificates, we have completed review of 64% and found the following: - 1,538: No Issues - 12: Errors

		Error reasons include spelling mistakes in information in the organization name, imprecise values in locality (related to the name change of Distrito Federal to Ciudad de Mexico), and any cases where we did not receive sufficient documentation to substantiate subject information. These certificates were revoked within 24 hours. We will provide crt.sh links to the revoked certificates.