**Issue D: URI in CN and dnsName SAN (December 2016)**

This certificate has a CN and dnsName value of "http://ripac.insopesca.gob.ve". RFC 5280, Section 4.2.1.6, says that dNSName values consist of letters, digits and the hyphen, and that excludes ":" and "/". A URI is not the same thing as an FQDN. Also, there is a SAN type for URIs, uniformResourceIdentifier. (Although using this would be forbidden under the BRs.)

This issue was reported to PROCERT on 7th August by email, and 16th August by bug report. This particular certificate was issued in Dec 2016 and was revoked on 11th August.

**PROCERT Response**

PROCERT initially claimed that this was entirely RFC-compliant, a claim comprehensively rebutted by Ryan Sleevi.

PROCERT then said: "Based on internals test and validation, we contacting the client, we asking for a new CSR and proceed to revoke and reissue the certificate, supporting into the installation process. We completed those actions in this point."

This certificate was issued with the modifications and here it is possible to appreciate the evidence [**https://crt.sh/?id=209727657**](https://crt.sh/?id=209727657)

**Issue E: Issuance of 1024-bit Certificate (December 2016**)

This certificate, issued on Dec 12 2016 for the purposes of OCSP signing, contains a 1024-bit key. PROCERT claimed that they have not issued certs with 1024-bit keys since 2010; once this example was pointed out, they corrected that to say "for end users". They have been asked whether they have issued any more certs with 1024-bit keys for any purpose, but have not yet responded.

**PROCERT Response**

PROCERT said: "Based on internals test and validation, we contacting the client, we asking for a new CSR and proceed to revoke and reissue the certificate in 2048, supporting into the installation process. We completed those actions in this point." They also said: "A deadline has been set until the 14th of this month to revoke and re-issue certificates with problems."

**Further Comments**

According to crt.sh, contrary to PROCERT's assertions, this certificate has still not been revoked as of 2017-09-18. And we are not sure who they are referring to when they say "the client", as this was a certificate for PROCERT's internal use for signing OCSP responses.

This certificate is not in use and is appended to the internal revocation schedule, the current certificate is 2048 in length and can be seen in the attached OCSP response (ocsp.txt)

**Issue G: Internal IP Address in SAN (March 2015 - March 20**17)

This certificate has an IP address value in SAN which is an internal IP address: 192.168.224.100. This is forbidden by the BRs section 7.1.4.2.1 and so the certificate should not have been issued.

This issue was reported to PROCERT on 12th August by email, and 16th August by bug report. The particular sample certificate was issued in March 2017 and was revoked on 24th August.

This certificate also has an IP address value in the CN and SAN which is an internal IP address: 10.79.6.100. While this cert has now expired, the notAfter date is later than the latest permitted notAfter date in the BRs for issuing certs with internal IPs, which was 1 Nov 2015.

This certificate was not issued by PSC PROCERT

**PROCERT Response**

PROCERT said: "Based on internals test and validation, we contacting the client, we asking for a new CSR and proceed to revoke and reissue the certificate, supporting into the installation process. We completed those actions in this point."

Please find evidence of new certificate issued without problems https://crt.sh/?id=202869851

**Issue I: CN Not Also In SAN (March 2016 - June 2017)**

The BRs section 7.1.4.2.2 a) require that the value in the CN also be in the SAN. This is to help the ecosystem deprecate the use of CN so it can eventually be ignored (because its semantics are unclear).

This certificate has a CN of "www.registroaba.cantv.net" but this value does not appear in the SAN. The SAN contains only "registroaba.cantv.net" and an IP address.

This issue was reported to PROCERT on 7th August by email, and 16th August by bug report. The certificate was issued in May 2017 and is still not revoked as of 28th August.

This certificate also has the same problem although, like many PROCERT certs, it was revoked on the day it was issued. This certificate and this certificate also have a CN which is not in the SAN. These are email certs not TLS certs, so the BRs do not apply, and this BR provision is not reflected in Mozilla policy. Still, it's not good practice, and it seems to be standard for PROCERT email certificates.

There are a total of 11 certificates with this problem.

**PROCERT Response**

PROCERT said: "Based on internals test and validation, we contacting the client, we asking for a new CSR and proceed to revoke and reissue the certificate, supporting into the installation process. We completed those actions in this point."

These certificates were revoked and generated again, please consult through the following link

<https://crt.sh/?iCAID=750&minNotBefore=2000-01-01&n=1000&cablint=25>

Issue I: CN Not Also In SAN (March 2016 - June 2017)

The BRs section 7.1.4.2.2 a) require that the value in the CN also be in the SAN. This is to help the ecosystem deprecate the use of CN so it can eventually be ignored (because its semantics are unclear).

This certificate has a CN of "www.registroaba.cantv.net" but this value does not appear in the SAN. The SAN contains only "registroaba.cantv.net" and an IP address.

This issue was reported to PROCERT on 7th August by email, and 16th August by bug report. The certificate was issued in May 2017 and is still not revoked as of 28th August.

This certificate also has the same problem although, like many PROCERT certs, it was revoked on the day it was issued. **This certificate and this certificate also have a CN which is not in the SAN. These are email certs not TLS certs, so the BRs do not apply, and this BR provision is not reflected in Mozilla policy. Still, it's not good practice, and it seems to be standard for PROCERT email certificate**s.

There are a total of 11 certificates with this problem.

**PROCERT Response**

PROCERT said: "Based on internals test and validation, we contacting the client, we asking for a new CSR and proceed to revoke and reissue the certificate, supporting into the installation process. We completed those actions in this point."

That certificate was revoked and generated again, please consult through the following link

[**https://crt.sh/?id=151828400&opt=cablint**](https://crt.sh/?id=151828400&opt=cablint)

**Issue J: Use of keyCertSign in Leaf Certificates (October 2016 - June 2017)**

24 PROCERT certificates have the Certificate Sign key usage bit set, but are leaf certificates. This is in contravention of the BRs 7.1.2.3 e).

**PROCERT Response**

PROCERT said: "The template for this certificate was fixed and based on internals test and validation, we contacting the client, we asking for a new CSR and proceed to revoke and reissue the certificate, supporting into the installation process. We completed those actions in this point."

Although certificates are not certified, the certificates have been revoked and corrected, please check the link

<https://crt.sh/?iCAID=750&minNotBefore=2000-01-01&cablint=782>

**Issue K: Internal DNS Names in Certificates (May - June 2017**)

This certificate has the following SAN values: "mail.fospuca.com, autodiscover.fospuca.local, autodiscover.fospuca.com, fospuca.local, fospuca.com, FOSPUCA-EXC.fospuca.local". Three of those are not resolvable in the public DNS, and therefore count as Internal Names under BRs section 7.1.4.2.1. This means the certificate should not have been issued.

Corrective action taken, please consult the link <https://crt.sh/?id=197158298&opt=cablint>

This issue was reported to PROCERT on 13th August by email, and 16th August by bug report. The certificate was issued in May 2017 and is still not revoked as of 28th August.

This certificate and this certificate and this certificate and this certificate also have an unqualified DNS name in the SAN, "OWASERVER", and the first of those is not revoked.

Corrective action taken, please consult the link <https://crt.sh/?id=197158298&opt=cablint>

**PROCERT Response**

PROCERT said: "Based on internals test and validation, we contacting the client, we asking for a new CSR and proceed to revoke and reissue the certificate, supporting into the installation process. We completed those actions in this point."

**Issue L: helloburgershack.com (June - July 201**7)

PROCERT seems to have made a large number of attempts at issuing certs for various domains under "helloburgershack.com" in June and July 2017.

The first one has an internal name among the SANs, "OWASERVER". The second one seems identical to the first. The third one changes the CN and the corresponding SAN value, but is otherwise the same. The fourth one is the first to still be unrevoked. It still contains the OWASERVER internal name, and again changes the CN and corresponding SAN value. The fifth and last one is also unrevoked. It had a typo in the email address and the organizationalUnitName. That makes it unlikely that the email address was properly validated; helloburgershack.co is not found in the DNS. It replaces the internal name OWASERVER with a second copy of "helloburgershack.com" in the SAN, so has duplicate SAN values.

We would be interested to know the sequence of events which led to this succession of certificate issuances.

**PROCERT Response**

PROCERT said on Friday 8th September: "Based on internals test and validation, we contacting the client, we asking for a new CSR and proceed to revoke and reissue the certificate, supporting into the installation process. This client provides a production window after the next Tuesday [12th September] in order to proceed with the revoke and the reissue of the certificate. Pending action." They also said: "A deadline has been set until the 14th of this month to revoke and re-issue certificates with problems."

That certificate was revoked and generated again, please consult through the following link <https://crt.sh/?id=167929373>

Further Comments

The fifth certificate, with typos, is still not revoked as of Monday 18th September.

That certificate was revoked and generated again, please consult through the following link [**https://crt.sh/?id=167929373**](https://crt.sh/?id=167929373)

**Issue M: CPS not in RFC 3647 or RFC 2527 Format (2011 - August 2017)**

RFC 3647, an update to RFC 2527, defines a format for CPS documents. The Baseline Requirements, section 2.2, require that a CA's CPS be in one of these two formats. (RFC 3647 has been around for 14 years; one would expect almost all CPSes to be in that format by now.) This is particularly important when, as in this case, the CPS is not in English, because the format gives guidance as to where to look for provisions on a particular topic and so one does not have to have the entire document translated.

However, neither PROCERT's CP nor CPS is in RFC 3647 or RFC 2527 format.

**PROCERT Response**

PROCERT said: "After a validation process, we modify the RFC number in our documentation. We complete this point."

Further Comments

We believe PROCERT has misunderstood this issue. The issue here is not that some RFC number in the document is wrong, but that the document is not arranged according to the layout given in RFC3647. To fix this would require completely rearranging the document, which we have seen no evidence that PROCERT have done.

This is not an infringement or violation of the RFC. Regarding to the language, the national language in Venezuela is the Spanish. We will work to updated the English version of this document and posted in the web page.

[**https://www.procert.net.ve/documentos/AC-D-0011.pdf**](https://www.procert.net.ve/documentos/AC-D-0011.pdf)

[**https://www.procert.net.ve/documentos/AC-D-0003.pdf**](https://www.procert.net.ve/documentos/AC-D-0003.pdf)

Standard

[**https://tools.ietf.org/html/rfc3647**](https://tools.ietf.org/html/rfc3647)

[**https://tools.ietf.org/html/rfc2527**](https://tools.ietf.org/html/rfc2527)

**Issue N: otherNames in Certificate SAN (2011 - August 2017)**

This certificate, and approximately 111 other certificates issued by PROCERT, have otherName entries in the list of Subject Alternative Names. This is forbidden by the BRs section 7.1.4.2.1, which states the only permissible types of SAN are dNSName and iPAddress.

PROCERT claim that "The first Other Name ... corresponds to the RIF (company tax number in Venezuela) of the contracting company, [due to] a formal request from SUSCERTE (Venezuela Government Agency) and is regulated in our corresponding CPS and CP. The second Other Name corresponds to the primary DNS of the DNS registered by the contracting company, both are regulated by the OID registry and in our CPS and CP."

The BRs contain a mechanism, in section 9.16.3, for a CA to violate the BRs when under compulsion of regulation, which might apply in this first case. However, this requires them to document the issue in their CPS section 9.16.3, and notify the CAB Forum by emailing questions@cabforum.org. It appears that neither of these things has been done, although the waters are muddied by the fact that the CPS is not in English and is not organized according to RFC 3647.

This issue was reported to PROCERT on 13th August by email, and 16th August by bug report. The particular sample certificate was issued in May 2017 and is still not revoked as of 28th August.

**PROCERT Response**

PROCERT said: "Based on internal testing and validation, we contact the customer, request a window to generate a new CSR and review and reissue the certificate, we will also support the installation process. We keep in touch with customers with active SSL to proceed with this point. We advance as much as possible with customers. Some of these certificates have expired. For the issue of new certificates, verify the observations contained in the number V."

Taking into account what the Baseline says, it states the following:

i. Other Subject Attributes

All other optional attributes, when present within the subject field, MUST contain information that has been verified by the CA.

Indicates that another field can be included as long as it is information verified by the CA in this case the CA verifies the number of RIF of each company and also the field is with an OID for that purpose, which is 2.16.862.2.2

**Issue O: OCSP Servers Return "Good" for Non-Existent Certificates (Unknown - August 2017)**

PROCERT's OCSP responder returns an OCSP status of "Good" for unknown certificates. This has been a violation of BR section 4.9.10 since 1st August 2013. This requirement was introduced due to the problems at Diginotar; an attacker issued certificates their system did not know about, and their OCSP responder called them all "good". Therefore, it is not an insignificant requirement.

This "good" OCSP response is for the serial number badca000badca000badca000badca000badca000badca000badca000badca000badca000badca000badca000badca000badca000badca000badca000, which is unlikely to correspond to an issued certificate.

Initially, PROCERT claimed that everything was fine because their responder returned the correct response for existing certificates and, later, that it returned "unauthorized" when asked about a certificate PROCERT had not issued. But it has been clearly demonstrated that for unknown certificates where the request claims PROCERT is the issuer, the response is incorrect.

**PROCERT Response**

PROCERT gave the following statement:

As we explained into Mozilla Bug (bug 1391058), when we applied the Microsoft tool, the system shows this message “In the Value data box, type the path to the directory you created in step 3 of the directory structure procedure and that contains the issued serial numbers, and then click OK.”.

We refresh or restart the service, then, the OSCP registry is automatically deleted. For testing we use different versions of Windows Server (2008, 2012 and 2016) all the versions present the same result. Additionally, we ask for an answer at Microsoft TechNet please https://social.technet.microsoft.com/Forums/windowsserver/es-ES/981f6e48-dc25-4eeb-a1d6-0bc72b9b4fc9/ocsp-online-responder-service-assume-a-certificate-that-is-not-included-in-the-crl-as-a-valid-and?forum=winserversecurity

Our OCSP works without any problem in the validation with automatic tools such as certutil, even with the same command openssl, in consultation under standard.

The standard openssl query is done in the following way: openssl ocsp -issuer issuer.cer -cert cert.cer -url http://ura.procert.net.ve/ocsp -noverify -text.

We detected that OCSP does work correctly with the Microsoft tool.

Open SSL creates a problem when doing a non-standard query (hacking). We are already working the point with Microsoft and we even have an assigned ticket.

Issue P: Use of SHA-1 To Sign OCSP Responses (Unknown - August 2017)

PROCERT OCSP responses are signed with SHA-1 and, since they reflect an attacker-controlled serial number, is vulnerable to a chosen prefix attack. This is not formally against documented policy but in the April 2017 CA Communication, PROCERT affirmed that "SHA-1 certificates are no longer used in the infrastructure related to our root certificates included in Mozilla's CA Certificate Program. (e.g. SHA-1 is no longer used to sign OCSP responses)." They asserted something similar in the March 2016 CA Communication. However, this appears not to be true.

PROCERT Response

PROCERT said: "We check the standard, the OCSP certificate is SHA 256, the answer in this case is an observation. We work to check and validate the adjust to SHA 256 in the OCSP answer. This situation does not contravene any standard."

No RFC 2560 nor RFC 5280 is being violated.

**Issue R: Incorrect Encoding of or Inappropriate Use of TeletexString (December 2015 - August 2017)**

TeletexString is one (deprecated) way of encoding string values in a certificate. Lots of PROCERT certificates (1, 2, 3) have got the encoding wrong. For example, This certificate has an incorrectly encoded TeletexString in Certificate and in X520LocalityName. This certificate uses an incorrectly-encoded TeletexString in X520OrganizationalUnitName, as do several other certificates.

These certificates were revoked and generated again, please consult through the following link <https://crt.sh/?iCAID=750&minNotBefore=2000-01-01&cablint=217>

This certificate is using TeletexString in the commonName, which is "\*.movilnet.com.ve", so that seems unnecessary as no special characters are required, and it's not the case for most other PROCERT certs.

The certificate was revoked and reissued, please see the link

[**https://crt.sh/?id=194225991**](https://crt.sh/?id=194225991)

**PROCERT Response**

PROCERT said: "Based on internal testing and validation, we contact the customer, request a window to generate a new CSR and review and reissue the certificate, we will also support the installation process. We keep in touch with customers with active certificate to proceed with this point. We advance as much as possible with customers

**Issue S: Non-Random Serial Numbers (September 2016 - August 2017)**

The BRs (section 7.1, since September 2016) and Mozilla Policy (section 5.2, since February 2017) require that every certificate contain at least 8 bytes (64 bits) of randomness in the serial number, as a preventative measure against hash algorithm weakness. Certificates currently issued by PROCERT, such as this example, seem to have serial numbers of the form of four leading bytes which are a time-based counter (measures in milliseconds), then zeroes, then a 2-byte incrementing per-cert counter. This practice is ongoing, although PROCERT confirmed in their response to Action 3 of the April 2017 CA Communication that they would conform to version 2.4.1 of the Mozilla Policy by June 1st, 2017. The question specifically mentioned the issue of 64-bits of randomness in serial numbers.

**PROCERT Response**

PROCERT said: "We check the observation. Procert technical staff applied the observation and fix the system in this particular point."

Already it was given previous answer to this point and was solved modifying certain parameters in our CA, which counts on a CSPRNG that acts like generator of serial numbers and was modified in its register so that it increased the capacity and strength of the serial numbers that generates automatically and without human intervention.

**Issue T: Inappropriate Key Usage Value of "Key Agreement" (October 2016 - August 2017**)

This certificate and 21 others all have a Key Usage of, among other things, "Key Agreement", which is inappropriate for an RSA public key. Many of these were revoked soon after they were issued. If the first ones were a problem, why was the problem not fixed? cablint marks this as an error, as it's a violation of RFC 3279 section 2.3.1.

**PROCERT Response**

PROCERT said: "The template for this certificate was fixed and based on internals test and validation, we contacting the client, we asking for a new CSR and proceed to revoke and reissue the certificate, supporting into the installation process."

These certificates were revoked and generated again, please consult through the following link <https://crt.sh/?iCAID=750&minNotBefore=2000-01-01&n=1000&cablint=734> Additionally, we have already modified the certificate template to prevent it from containing this key usage.

**Issue V: Failure to Respond Quickly To Problem Reports (August 2017)**

Jonathan Rudenberg submitted problem reports to PROCERT regarding some of the issues in this list:

Issue D (URI in CN and dnsName SAN): reported 7th August; cert revoked 11th August

Issue I (CN not also in SAN): reported 7th August; cert not yet revoked

Issue G (Internal IP Address in SAN): reported 12th August; cert revoked 24th August

Issue K (Internal DNS Names in Certificates): reported 13th August; cert not yet revoked

PROCERT did not provide a direct answer to the question in the last major CA Communication regarding a Problem Reporting Mechanism; they simply pointed at their CPS. Jonathan used the email address "contacto@procert.net.ve", which appears in that CPS and is also a contact address supplied by PROCERT to Mozilla for official communications from the Root Program, so we consider these reports to have been validly submitted.

Jonathan did not receive any direct response from PROCERT to his reports. While the BRs currently contain no requirement to respond to the problem reporter within any time period, they do contain a requirement to revoke misissued certificates within 24 hours. This clearly did not happen in any of the cases above. Mozilla allows some unofficial leeway in this based on an assessment of the security risk, if there is careful published analysis and a timeline is given for revocation. That has not happened in this case.

**PROCERT Response**

PROCERT said: "We tested our certificates in our test environment, we analyze the issues and apply measure to solve the issues, later, the team takes actions, modify certificates templates, work in the CA, made test, generated new certificates in our internal environment. Then contacted the clients and agree a revocation date, revoke all the certificates with problem and reissue the certificates with the standard complying, check the correct application of CA Browser Forum, implant a regular training program (including test (operational and theory) to our staff in order to prevent and solve any issue, finally proceed with a dismissal of one operator."

**Issue W: Test Certificates Issued in Publicly Trusted Hierarchies (August 2017)**

This certificate and this certificate have "test" values in the CN, OU and stateOrProvinceName. They have the emailProtection EKU but no email address in the CN or SANs.

**PROCERT Response**

PROCERT said: "The certificate was revoked and we put enforce our security policy in order to prevent futures events. Also we instruct our operational staff regarding internal process and IT Security topics".

This action does not infringe any standard, in any case by security policy should not be issued for a long time, since despite having a quality environment, you can always test in the production environment some test certificate, all the certificates were revoked and were only issued under an authorization, since for the issuance of certificate there is a mechanism of approval of 3 levels, In addition the certificates were revoked

<https://crt.sh/?id=197073488&opt=cablint>

<https://crt.sh/?id=197155020&opt=cablint>

**Issue X: High Percentage of Revocations (August 20**17)

Large proportions of the certs issued by PROCERT and known to CT are revoked almost immediately. Looking just at the start of August, we see: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13.

While this is not against any policy, it does seem strange. Is there something wrong with these certificates? If so, what, and why has the problem not been fixed?

**PROCERT Response**

PROCERT said: "Staff takes actions considering the observations includes into the Mozilla bug. In order to that, we made an internal audit, check the issuance process, detected al the unconformities, contacting the clients, agree with the clients a windows to revoke and installing the new certificates. In order to duly comply, we proceeded to revoke certificates with observations (Mozilla Bug). We planning replace all the certificates with observations. That why you can appreciate a high percent into the certificates revocations".

**Further Comments**

The issue being raised here is not the large number of certificates that PROCERT is revoking (we might expect a large number of revocations, given all of the problems), but the fact that a large number are revoked very shortly after they are issued. Why does that keep happening? If they are being issued incorrectly, why are corrective steps not being taken?