



| | | |
|---|---|--|
|  | <p style="text-align: center;">PROVEEDOR DE CERTIFICADOS (PROCERT), C.A. ADD PROCERT AC CERTIFICATE AS TRUST ANCHOR ATTACHMENT MOZILLA BUG 593805 Comment 86</p> | <p>Revision Nº 1 Month and Year 01/22/2013</p> |
| Senior Management | Document | Edition 1 |


| ITEM | INFO NEEDED | Mozilla Questions and PROCERT Answers |
|------|--|--|
| 1 | <p>Please add a comment to this bug to provide your response to the action items listed in the CA Communication that was sent today, and is available here: https://wiki.mozilla.org/CA:Communications#January_10.2C_2013</p> | <ol style="list-style-type: none"> 1. Mozilla: Review the proposed changes to Mozilla’s CA Certificate Policy, and assess the impact of those changes to your CA operations. Procert: The proposed updates to Mozilla’s CA Certificate Policy do not require further change to our CA operations, because our CA operations already comply with the proposed policy. 2. Mozilla: Confirm compliance with the CA/Browser Forum’s Baseline Requirements. The CA/Browser Forum (http://www.cabforum.org) released the "Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates," which became effective on July 1, 2012. It is our expectation that as of January 2013 CA issuance of SSL certificates will be audited against these Baseline Requirements as well as the acceptable audit criteria that are listed in Mozilla’s CA Certificate Policy. Procert: Our CA operations conform to the CA/Browser Forum’s Baseline Requirements for issuance of SSL certificates, and our next audit will include verification of this conformance. 3. Mozilla: Scan your certificate database for certificates that incorrectly have basicConstraints with the cA boolean set to true, or are incorrectly enabled with the keyCertSign Key Usage bit. Due to the recent incident in which a mis-issued intermediate certificate was found (https://blog.mozilla.org/security/2013/01/03/revoking-trust-in-two-turktrust-certificates), we are concerned that CAs may have responded to |

| | | |
|---|---|--------------------------------|
| <p>Made By: Senior Management Operational Staff Date: 01/21/13</p> | <p>Approved by: Senior Management Director Appointed – Oscar Lovera Date: 01/22/13</p> | <p>Page 1 de 4</p> |
|---|---|--------------------------------|

| | | |
|---|---|--|
|  | <p style="text-align: center;">PROVEEDOR DE CERTIFICADOS (PROCERT), C.A. ADD PROCERT AC CERTIFICATE AS TRUST ANCHOR ATTACHMENT MOZILLA BUG 593805 Comment 86</p> | <p>Revision Nº 1 Month and Year 01/22/2013</p> |
| Senior Management | Document | Edition 1 |


| | | |
|--|--|--|
| | | <p>our last communication based on their policies, rather than checking their certificate databases. Therefore, we request that you scan your certificate database and inform Mozilla if you find any un-expired intermediate certificates in your CA hierarchy that should not be trusted. In your reply, please attach all such intermediate certificates, even if you have already revoked them. While you are scanning your certificate databases to ensure that all certificates with basicConstraints:CA:TRUE have been issued in accordance with your CPS, please also check for compliance with the following practices.</p> <ul style="list-style-type: none"> • All certificates with basicConstraints:CA:TRUE have the basicConstraints marked critical. • All intermediate certificates with basicConstraints:CA:TRUE have cRLDistributionPoints containing a well-formed and compliant URL that returns a valid CRL. • All certificates that share a common issuer name contain unique serial numbers (independent of certificate expiration). • All end-entity certificates with RSA key sizes smaller than 2048 bits expire no later than December 2013. • Certificates are not issued with sequential serial numbers. If it is found that certificates have been issued with contiguous serial numbers, then the subject of those certificates must contain unpredictable data that is not under the control of the certificate subscriber. <p>Procert: We have scanned our certificate database, and confirm that</p> |
|--|--|--|

| | | |
|---|---|--------------------------------|
| <p>Made By: Senior Management Operational Staff Date: 01/21/13</p> | <p>Approved by: Senior Management Director Appointed – Oscar Lovera Date: 01/22/13</p> | <p>Page 2 de 4</p> |
|---|---|--------------------------------|

| | | |
|---|---|--|
|  | <p style="text-align: center;">PROVEEDOR DE CERTIFICADOS (PROCERT), C.A. ADD PROCERT AC CERTIFICATE AS TRUST ANCHOR ATTACHMENT MOZILLA BUG 593805 Comment 86</p> | <p>Revision Nº 1 Month and Year 01/22/2013</p> |
| Senior Management | Document | Edition 1 |

| | | |
|--|--|---|
| | | <p>there are no un-expired intermediate certificates in our CA hierarchy that should not be trusted. We have also checked our certificate database to confirm that all of the non-expired certificates have been issued in accordance with the listed practices.</p> <p>4. Mozilla: Deprecate issuance of SSL certificates containing a Reserved IP Address or Internal Server Name. The CA/Browser Forum's Baseline Requirements state: "As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA SHALL notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016." This practice is being eliminated for security reasons, so we encourage all CAs to begin working with their customers to transition to alternative arrangements, and to stop issuing SSL certificates containing Reserved IP Addresses or Internal Server Names as soon as possible rather than waiting until the deadline. Procert: We do not issue SSL certificates that chain up to a root certificate that is included in Mozilla's CA Certificate Program and that contain Reserved IP Addresses or Internal Server Names.</p> <p>5. Mozilla: For each root certificate or trust anchor you control that is included in Mozilla's CA Certificate Program and has the SSL trust bit enabled by default, please provide a URL to a website (which may be a test site) whose SSL certificate chains up to it. We expect this website to</p> |
|--|--|---|

| | | |
|---|---|--------------------------------|
| <p>Made By: Senior Management Operational Staff Date: 01/21/13</p> | <p>Approved by: Senior Management Director Appointed – Oscar Lovera Date: 01/22/13</p> | <p>Page 3 de 4</p> |
|---|---|--------------------------------|

| | | |
|---|---|--|
|  | <p style="text-align: center;">PROVEEDOR DE CERTIFICADOS (PROCERT), C.A. ADD PROCERT AC CERTIFICATE AS TRUST ANCHOR ATTACHMENT MOZILLA BUG 593805 Comment 86</p> | <p>Revision Nº 1 Month and Year 01/22/2013</p> |
| Senior Management | Document | Edition 1 |

| | | |
|--|--|---|
| | | <p>endure for the lifetime of the root, or until you notify us of an alternative URL. The website does not need to support high traffic loads or have greater than 99% uptime. Procert: https://mail.procert.net.ve/exchange</p> |
|--|--|---|

CONFIDENCIAL - NO COPIAR - PROPIEDAD DE PROCERT

| | | |
|---|---|--------------------------------|
| <p>Made By: Senior Management Operational Staff Date: 01/21/13</p> | <p>Approved by: Senior Management Director Appointed – Oscar Lovera Date: 01/22/13</p> | <p>Page 4 de 4</p> |
|---|---|--------------------------------|