KPMG

AGESIC

Audit service for Autoridad Certificadora Raíz Nacional

SP No 03/2016

Deliverable 4: Audit procedures results in English

KPMG

February 14th, 2017

To AGESIC: Our Ref.: 2250.69

Montevideo, February 14th, 2017

According to our proposal, we have performed audit procedures regarding Autoridad Certificadora Raíz Nacional's (ACRN) operation.

Our service includes performing several activities with the objective of executing audit procedures on the infrastructure, policies and procedures of the ACRN using the *Trust Service Principles and Criteria for Certification Authorities 2.0 international standard (ex WebTrust)* as a reference framework. The scope of our review was ACRN's self-signed root certificate with SHA-1 thumbprint 7A:1C:DD:E3:D2:19:7E:71:37:43:3D:3F:99:C0:B3:69:F7:06:C7:49, during the period from December 1st, 2015 through December 1st, 2016.

As a result of our work, we have delivered the following reports:

1. Adjusted work plan
2. Preliminary results
3. Audit report
4. Audit report in English

This report corresponds to deliverable 4: Audit report in English.

As a result of our activities, we have not identified any situations that would result in a significant deviation from the Trust Service Principles and Criteria for Certification Authorities 2.0 standard. However, we have detected observations and improvement opportunities which are outlined in the Results section of this document.

This report is for the exclusive use of AGESIC and it shall not be distributed to third parties, mentioned nor referenced, in part or as a whole, without our written consent.

We remain at your disposal to provide additional information and clarification, as required.

Sincerely,

KPMG

Cr. Rodrigo Ribeiro
Partner

Activities performed

The following activities have been performed in order to elaborate this deliverable:

- Visit to the primary datacenter, located at AGESIC
- Visit to the secondary datacenter, located at ANTEL Pocitos
- Meetings with ACRN operators
- Critical reading of ACRN's policies and procedures (CP and CPS)
- Analysis of policies and procedures, such as, but not limited to:
    - Security Policy
    - Internal Procedures Manual
    - Log Review Procedure
    - Disaster Recovery Plan

The result of the execution of these activities is described in the following pages, including findings and improvement opportunities.

Main findings

Our main findings are included below. These findings are the result of the execution of the activities described above.

Certification Practice Statement (CPS)

As a result of our critical reading of the ACRN's Certification Practice Statement (CPS) and our analysis of ACRN's web site at the time of our preliminary report, we found:

- The CPS does not include a periodic review procedure. ***This situation has been corrected during our work, in a new CPS version that includes an annual review.***
- ACRN's web site intends to include links to both CPS versions (as we can infer from the texts on the links). However, the link that should point to CPS version 2, actually points to the Certificate Policy (CP). A document containing the summary of changes in version 1.1 is also published, dated 17 April 2012. ***This situation has been corrected during our work.***

Certificate Policy (CP)

As a result of our critical reading of the ACRN's Certificate Policy (CP) at the time of our preliminary report, we found:

- The CP does not include a periodic review procedure. The ACRN's Security Policy establishes an annual review, but it has not been performed this often. **This situation has been corrected during our work, in a new version that includes an annual review.**
- The first CP version was approved on October 5th, 2011 and it was last updated on January 3rd, 2017.
- This last version of the CP includes a link in section 1.2 to where it is published online. However, this link points to the first version of the CP and not the current version. ***This situation has been corrected during our work.***
- This last version of the CP includes two links in section 7.1.10.1 "Políticas de Certificación (Certificate Policies)" that lead to the CPS posted on AGESIC and UCE's web sites. The first link that leads to UCE's web site, returns error 404 (not found). The second link leads to the first version of the CPS and not the current one. **This situation has been corrected during our work.**

CP and CPS Consistency

- At the time of our preliminary report, the CPS in section 4.3 stated that the certificate's duration will be 10 years, whereas in the same item of the CP it stated that *"the certificates' duration will be the timespan between the issued date and the ACRN's certificate due date, if the certificate is not revoked prior to this date..."*. This modification was approved by UCE's resolution number 002/13, file 2013-2-10-0000150, dated April 17th, 2013. Only the CP was modified. ***This situation has been corrected during our work. The new CPS version of the document is consistent with the CP wording.***

Physical Access to RootCA's facilities

Main findings:

- A fingerprint reader is installed at the RootCA's server room main entrance, but it is not operational.
- Cameras are installed inside the room, however there are no cameras installed on the outside, pointing at the entrance door.

Disaster Recovery Plan

As a result of our critical reading of the ACRN's Disaster Recovery Plan (DRP) at the time of our preliminary report, we found:

- The key personnel list includes a member who is no longer an ACRN employee. ***This situation has been corrected during our work, in a new version of the DRP.***
- This plan does not require to be periodically tested or updated. ***This situation has been corrected during the execution of our procedures, in a new version of the DRP.***
- The list of operators who are authorized to enter the ACRN's secondary facilities contains an operator who is not an ACRN employee, but works at an authorized CA (Correo Uruguayo).

Compliance and monitoring

As a result of our critical reading of the ACRN's Policies and Procedures at the time of our preliminary report, we found:

- An audit log review procedure has been established. According to the evidence received, the last review had been performed on November 3rd, 2015. This procedure does not require a periodic execution. ***This situation has been corrected during our work, in a new version which states that log reviews must be performed at least annually.***

Information Security Management

As a result of our critical reading of the ACRN's Security Policy at the time of our preliminary report, we found:

- The Security Policy requires the RootCA's manager to perform periodic reviews of personnel activities to ensure they are able to manage certificates and keys. We have not received evidence regarding the execution of these reviews. ***This situation has been corrected during the execution of our procedures, in a new version that no longer requires this review process.***
- The Security Policy also states that the Security Officer is responsible for developing training programs and keeping record of their execution. Its responsibilities also include keeping records of the annual acceptance of the Security Policy. We have been informed that formal training programs have not been developed. ***This situation has been corrected during our work, a new version of the Policy which states that the RootCA's Manager must assess training needs, and the Security Officer and Network and Systems Administrator must conduct the training sessions.***

- At the time of our preliminary report, ACRN's Security Policy stated that:

    - *All RootCA systems that could be affected by viruses, trojans, worms, backdoors, rootkits or other malware, must be protected by an up to date antivirus solution.*
    - *Periodic software updates and full scans must be performed and records must be kept according to the Audit Log Policy.*

    We have not received evidence regarding the execution of these activities.

    This situation has been corrected during our work, in a new version of the document that states that due to the complexity involved in patch deployment on ACRN's production and backup systems, and the complexity involved in keeping an antimalware solution up to date on those systems, patches will be deployed when operational issues arise, and an antimalware solution will not be deployed on ACRN's systems.

- The Security Policy states that security patches must be deployed within 3 months. We have not received evidence regarding patch deployment. According to documentation received, RootCA's servers run on CentOS v5.6, which no longer receives full updates (only security updates), and its support is scheduled to end on March 31st, 2017. ***This situation has been corrected during our work, in a new version of the document which states that the only updates that will be deployed are the ones that patch functionalities that affect ACRN's operation.***

- The Security Policy states that password maximum age must be 90 days, enforcing a password history that disallows reusing the last 5 passwords. However, we received an approved Change Request that sets the maximum password age to 365 days. ***This situation has been corrected during our work, in a new version of the document which states that the password's age is set to 1 year and a password history of 5 passwords is kept.***

- It was stated that:

    - *"The physical security measures that the data processing facilities must have are at least the following…"*
    - *One of the measures required is the following: "Card readers or fingerprint readers that control and log access to sensitive areas inside the ACRN's facilities."*

    During our visit we could verify that a fingerprint reader and a magnetic lock are installed but not operational. ***This situation has been corrected during our work, in a new version of the document which no longer requires the use of card readers or fingerprint readers.***

- The Security Policy states that the document and the CP must be reviewed annually, in conjunction with CERTuy. We have not received evidence of the execution of these reviews in the past year. ***This situation has been corrected during work, in a new version of the document, dated January 11th, 2017.***

- It is stated that all personnel that will be hired must comply with the RootCA's Security Policy in writing and accept its duties and responsibilities by signing the Security Policy

Acceptance Form. Besides, the RootCA's Confidentiality Agreement must be signed. We have not received evidence that the external employee who works at Correo Uruguayo has signed the Confidentiality Agreement.

- It is stated that when an employment contract is terminated, measures that prevent access to RootCA's facilities and systems must be taken, e.g. disallowing physical access on sensitive areas, recovering access keys or smart cards, or disabling user accounts.

  A Systems and Network Administrator has resigned. However, we have not received evidence of the execution of all the required actions, such as approved change requests regarding user account termination on ACRN's systems.

Our main findings arising from the critical reading of the ACRN's Procedure for Third-party Access to RootCA's Facilities are outlined below:

- "The external employee must sign the Request Form, detailing any situation that considers relevant about the visit.". According to the procedure, an external employee is a person or people that require access to RootCA's facilities.

  Although personal information was required to authorize our access, we were not required to sign the Request Form during our visit. ***This situation was corrected during our activities, in a new procedure dated February 9th, 2017 which no longer requires external employees to sign a Request Form.***

- The document states that the physical access control must generate independent records.

  Currently, the installed physical access control is a key lock, which does not generate records by itself. ***This situation was corrected during our work, in a new procedure dated February 9th, 2017 which no longer requires independent record generation.***