ANEXO III - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

ANEXO III

PROCEDIMIENTOS PARA LA AUTORIDAD CERTIFICANTE

1 INTRODUCCIÓN

1.1 GENERALIDADES

El presente documento establece los procedimientos de la Autoridad Certificante del Gobierno de la Ciudad de Buenos Aires para la firma y emisión de certificado, firma de solicitudes de revocación y firma y generación de CRLs.

Este documento está sujeto a las características y condiciones establecidas por la Política de Certificación de la PKI del Gobierno de la Ciudad de Buenos Aires.

Este Procedimiento asume que el lector conoce los conceptos básicos de PKI, certificado y firma digital, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento. En la dirección ac.buenosaires.gov.ar se pueden encontrar los conceptos generales y usos referidos a las firmas digital y electrónica.

1.2 Firma de solicitud y emisión de Certificado Digital

La Autoridad Certificante (CA) recibe de la RA las solicitudes de certificados de los suscriptores aprobadas y firmadas elect rónicamente por la propia RA.

1.2.1 Transferencia de las solicitudes hacia la CA

Para realizar la transferencia de las solicitudes firmadas electrónicamente desde la RA hacia la CA, se utilizará un dispositivo de almacenamiento externo, que será exclusivo para ese uso.

1.2.2 Firma de la solicitud de certificado

Seleccionando la solicitud deseada y una vez verificada la firma de la RA, se procederá a la firma de dicha solicitud que por intermedio de la conexión con el HSM y su certificado raíz, quien firmará y generara el certificado digital correspondiente al suscriptor.

1.2.3 Transferencia de los certificados hacia la RA

Para realiza r la transferencia de los certificados digitales, desde la CA hacia la RA, se utilizará un dispositivo de almacenamiento externo, que será exclusivo para ese uso.

ANEXO III - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

1.3 Firma de solicitud de revocación y emisión de CRL

La CA recibe de la RA las solicitudes de revocación de certificados de los suscriptores aprobadas y firmadas electrónicamente por la propia RA. Asimismo, la RA podrá solicitar la revocación de un certificado digital en caso de verificar que haya sido emitido en base a información falsa o si se determina que los procedimientos de verificación han dejado de ser seguros.

En estos últimos supuestos, deberá remitir requerimiento fundado firmado electrónicamente a la CA.

1.3.1 Transferencia de las solicitudes hacia la CA

Para realizar la transferencia de las solicitudes de revocación firmadas digitalmente desde la RA hacia la CA, se utilizará un dispositivo de almacenamiento externo, que será exclusivo para ese uso.

1.3.2 Firma de la solicitud de revocación

Seleccionando la solicitud deseada y una vez verificada la firma de la RA, se procederá a la revocación del certificado digital correspondiente al suscriptor.

1.3.3 Firma y generación de CRLs

Se deberá seleccionar la opción de generación de una nueva CRL y se procederá a la firma de dicha lista por intermedio de la conexión con el HSM y su certificado raíz.

1.3.4 Transferencia de la CRL

Para realizar la transferencia de la CRL firmadas digitalmente desde la CA hacia la RA, se utilizará un dispositivo de almacenamiento externo, que será exclusivo para ese uso.

1.3.5 Revocación de certificados

Si la CA determina que los procedimientos de seguridad o verificación dejaron de ser seguros o la información contenida en los mismos ha dejado de ser válida, podrá revocar los certificados digitales emitidos en estas condiciones.

En estos casos, deberá informar dichas circunstancias a través de correo electrónico a los suscriptores y a la máxima autoridad de la jurisdicción en donde se desempeñe el mismo.