Instituto Nacional Electoral

PREP 2015 MX

Programa de Resultados Electorales Preliminares

INFORME DE VIABILIDAD PARA EL USO DE MECANISMOS DE SEGURIDAD EN LA DIGITALIZACÓN DE ACTAS DE ESCRUTINIO Y CÓMPUTO

UNIDAD TÉCNICA DE SERVICIOS DE INFORMÁTICA

Febrero de 2015

Contenido

1. Escenario: Marcas de agua

1.1 Descripción del escenario

Se propone utilizar las marcas de agua digital a fin de garantizar la autenticidad e integridad de las actas digitalizadas durante la operación del PREP 2015.

Para integrar Marcas de Agua en el Proceso de Digitalización de Actas deberá llevarse a cabo un desarrollo que permita integrar de forma transparente el uso de marcas de agua en el proceso de digitalización.

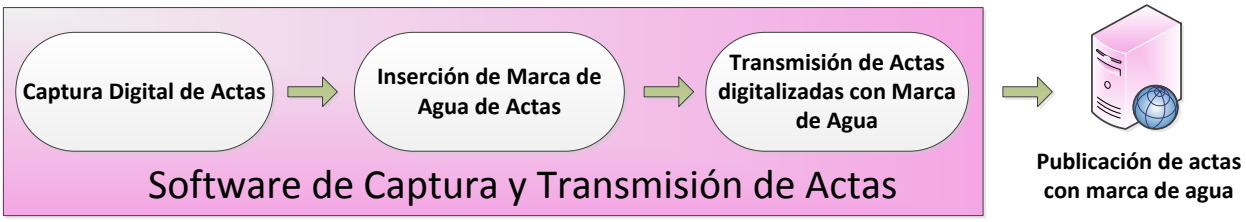

Figura 2. Esquema de inserción de Marca de Agua

1.2 Definición de Marca de Agua imperceptible

Es una técnica que inserta un código de identificación invisible, ya sea firma, marca, sello o contraseña en la información a proteger, posibilitando la identificación de la fuente, autor, propietario, e información como puede ser: la fecha de creación y si esta marca ha sido modificada. Donde su principal ventaja consiste en que la marca es inseparable del contenido del archivo.

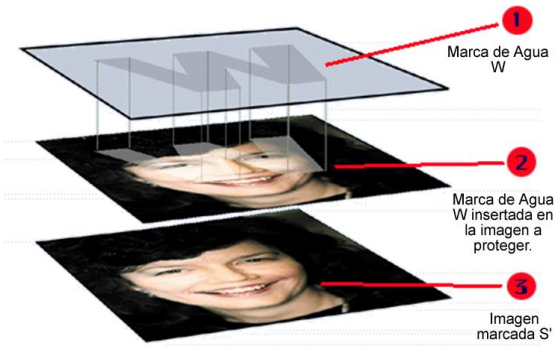

Figura 1. Esquema general Marca de agua imperceptible

El propietario de un medio digital debe de ser capaz de detectar cualquier intento de alteración ilegal de su trabajo, asegurado la integridad u originalidad del material marcado. En el mejor de los casos un solo bit alterado sobre el material marcado puede ser detectado.

1.2.1 Consideraciones para el uso de marcas de agua imperceptible

Esta opción no es viable en este momento debido a que la marca de agua invisible es un mecanismo que sobrepone información a la imagen original sin alterar como es percibida por el usuario, sin embargo en este momento presenta las siguientes complicaciones.

1. La mayoría de los algoritmos estenográficos devuelven una salida en BMP o PNG nuestro formato actual de digitalización es JPG.
2. Agregar información a la imagen implica reprocesarla para alterar los bits correspondientes lo que derivaría en un aumento en el tiempo de digitalización

Se necesitaría hacer o adquirir una aplicación capaz de decodificar la información adicional de la imagen.

1.3 Definición de Marca de Agua Perceptible

Las marcas de agua visibles son generalmente figuras que aparecen en el fondo de la imagen (documento) para autenticar e indicar quién es el propietario de los datos.

Para el ciudadano esta marca puede ser un distintivo de autenticidad al ver la imagen publicada, siempre y cuando se publique la imagen con la marca de agua.

1.3.1 Consideraciones para el uso de marcas de agua perceptible

Esta opción no es viable debido a que el proceso de marcado o de validación de la marca de agua por parte del aplicativo afecta en el rendimiento y desempeño de la aplicación. También se incrementan los tiempos de publicación debido al costo en el procesamiento de la imagen. Por último se puede presentar lentitud (costo computacional) en el proceso de marcado o de verificación de la marca de agua.

2. Escenario: Uso de firma digital en el código QR del acta digitalizada

2.1 Descripción del escenario

Para garantizar la integridad de las actas digitalizadas se propone firmar digitalmente la información de la casilla que esta almacenada en el código QR y almacenar el resultado de dicha firma dentro del mismo código QR.

Para integrar una firma digital en el código QR que se adhiere en las Actas de Escrutinio y Cómputo deberá llevarse a cabo un desarrollo que permita firmar digitalmente la información de la casilla.

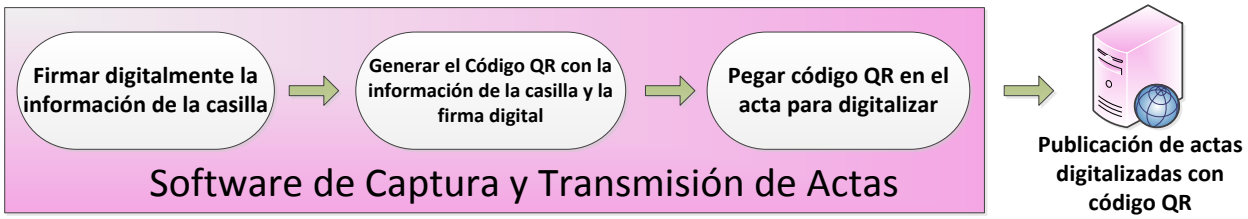

Figura 3. Esquema de generación de firma digital en código QR

Definición del código QR

Un código QR es la definición comercial de un método útil para almacenar datos de manera eficiente y que puedan ser leídos de forma automática por una aplicación de software.

Definición de firma digital

Una firma digital es un mecanismo criptográfico que permite determinar quién ha generado la información (imágenes, audio, video, etc.) y confirmar que dicha información no ha sido alterada desde el momento que se produjo la firma digital.

2.2 Consideraciones para el uso de firma digital el código QR

La posibilidad de utilizar el código QR para almacenar el resultado de la firma digital de los datos de las casillas tiene como desventaja que una vez digitalizada el acta la región donde se ubica el código QR puede ser manipulada y se puede sustituir por cualquier otra imagen de código QR. Mediante este esquema no es posible garantizar la integridad del acta que ha sido

digitalizada, por lo tanto no proporciona certeza de que el acta no ha sido manipulada por un tercero.

3. Escenario: Código de integridad.

3.1 Descripción del escenario

Obtener el código de integridad de cada una de las actas digitalizadas y publicarlo en internet junto con cada una de las actas digitalizadas.

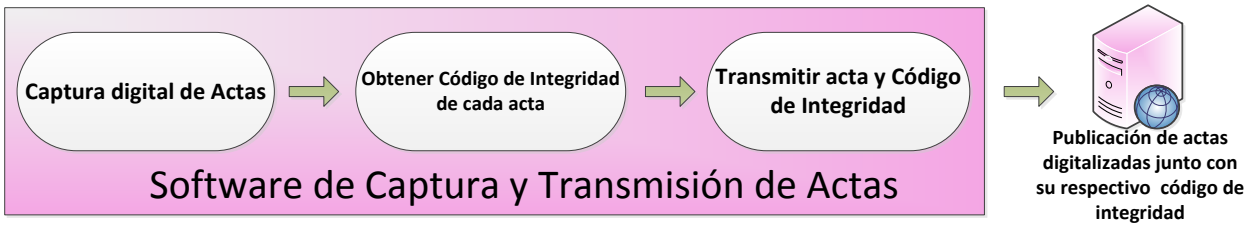

Figura 4. Esquema de generación código integridad SHA

Definición del código de integridad

Un código de integridad o función hash es un algoritmo que transforma un conjunto de datos en único valor de longitud fija. Si el conjunto datos originales es modificado la salida de la función hash es diferente lo que permite identificar que la información ha sido modificada y por lo tanto ha perdido la característica de integridad.

3.2 Consideraciones para el uso de código de integridad

Esta opción es viable debido a que actualmente ya se genera el código de integridad al momento que son digitalizadas las actas. Esta tecnología permite identificar que la imagen digital ha sido altera aunque no es posible identificar la región que ha sido modificada.

4. Conclusiones.

Respecto de las marcas de agua imperceptible, esta opción no es viable debido a la complejidad técnica que implica su desarrollo y su implementación impacta ampliamente lo que ya ha sido desarrollado hasta el momento.

En relación a las marcas de agua perceptibles, no es viable debido al costo computacional requerido y que esto impacta directamente en la velocidad de digitalización y como consecuencia se incrementa el tiempo de publicación de las actas.

Por otro lado, el uso de la firma digital dentro del código QR no aporta garantías que permitan asegurar la integridad de las actas digitalizadas.

Por último generar el código de integridad SHA se ha utilizado en años anteriores y está actualmente implementado. Esta tecnología garantiza la integridad de las actas.

Todas las tecnologías analizadas en este documento son de difícil comprensión para el ciudadano común. Se requeriría publicar en el sitio del PREP 2015 información y orientación a los ciudadanos sobre el uso de estas tecnologías.