

## Objetivo

Generación de prototipo de urna electrónica, para registro de votos.

## Propuesta técnica

### Consideraciones:

La urna electrónica será un sistema auto contenido, sin conexión a alguna fuente de datos externa, y no realizará tareas de ningún tipo relacionadas con la manipulación de los datos ahí almacenados o por almacenar (debiéndose entender por esto: consultas, modificaciones, eliminaciones). Los resultados solo se podrán imprimir a través de las opciones que se le incorporen a la interfaz del sistema, con los fines establecidos para los propósitos aquí declarados y de acuerdo a lo que el IEC pudiera determinar.

La urna electrónica utilizará como medio de control para emisión del voto tarjetas PVC con tecnología NFC (de ahora en adelante referidas como tarjeta NFC).

La tarjeta NFC contendrá una cadena digital única (de ahora en adelante referida como token) para habilitar el registro del voto.

El token será envuelto con un algoritmo de cifrado tradicional para que, en caso de que la tarjeta NFC fuera extraída de la casilla y leída por algún dispositivo, el contenido del token esté protegido.

El token estará compuesto de múltiples partes: datos Identificadores de hardware y software obtenidos de la computadora, "timestamp" o sello de tiempo que contiene información de la fecha y hora de un momento determinado y datos de la casilla, con la intención de que garanticen la unicidad de la cadena; la segunda parte es el folio que le correspondería a la boleta, lo que generaría un identificador único en cada ocasión que se vaya a emitir un voto.

La primera parte de la cadena se generaría al momento de configurar la urna electrónica durante la preparación de la casilla, y sería sincronizada en ese instante con los dos lectores de tarjeta NFC mediante conexión física USB, sin que esta conexión vuelva a ser requerida durante la jornada electoral.

El token compartido entre la computadora y los lectores de tarjetas NFC garantizará que esa tarjeta NFC solo pueda ser utilizado únicamente en esa urna electrónica, además de que validará que el elector solo pueda votar una sola vez en cada uno de los cargos.

Las tarjetas NFC originalmente se encontrarán desactivada, y solo se activarían cuando el presidente de la casilla valide que el elector pueda votar según los documentos establecidos para ese efecto (lista nominal, adicional o resolución favorable de la instancia correspondiente según el procedimiento electoral). Una vez registrada la intención del voto en la urna electrónica la tarjeta se desactivaría y debería ser devuelta al presidente de la casilla. Cada vez que el presidente active la tarjeta NFC, la misma contendrá el token y un folio único, consecutivo **e irrepetible**.

La información que se genere en la urna electrónica no podrá ser asociada con el padrón electoral puesto que la urna electrónica solo registrará los voto asociados al folio, por cargo.

## Metodología

La solución de software contempla dos etapas:

- 1) Pre configuración de la urna electrónica. Previo a la jornada electoral, el instituto electoral realizará esta tarea en la cual se registrará la información correspondiente a los partidos políticos y/o candidatos participantes, representantes de partidos, etc., partiendo en un archivo XML de estructura definida para ese propósito que contendría dicha información para evitar el registro de esos datos como parte de la jornada electoral.
- 2) Jornada electoral. Relativa a los momentos de la jornada electoral y comprende:
  - a. Preparación e instalación de la casilla.
    - i. El presidente de casilla se registrará, debiendo generar una contraseña para operar los espacios seguros del proceso, y luego proceder a registrar los funcionarios de casilla. Se imprime un comprobante de la operación.
    - ii. El presidente procede a inicializar la casilla, para lo cual registrará entre otra información los folios asignados a la casilla, generándose automáticamente una cadena única en ese momento con datos de la computadora, así como datos de la casilla. La firma electrónica digital cifrada generada será compartida entre la urna y las terminales lectoras de tarjetas NFC en ese momento a través de un cable USB. Al final se imprimirá un comprobante que contenga la información correspondiente, de acuerdo a lo establecido por el IEC, al acta de apertura de casilla debiendo comprobar que todos los registros relacionados con la votación se encuentran en cero.
  - b. Votación.
    - i. El presidente solicita la credencial para votar y sigue los procedimientos establecidos por el IEC para verificar que no haya votado previamente.
    - ii. Después de determinarse favorablemente que el elector se encuentra en lista nominal o lista adicional o cuenta con resolución favorable de la instancia correspondiente según el procedimiento electoral, el presidente toma una tarjeta NFC y la coloca sobre la unidad de escritura de tarjeta NFC para activarla y asignarle un token válido.
    - iii. El elector se dirige a la urna electrónica.
    - iv. El elector coloca la tarjeta NFC en la unidad lectora de tarjeta NFC
    - v. La urna electrónica lee y valida el token contenido en la tarjeta NFC.
    - vi. Si el token en la tarjeta NFC es válido, se repetirán los siguientes pasos por cada cargo de elección de la jornada electoral
      - a) La urna presenta en pantalla los múltiples candidatos al cargo
      - b) El elector marca su(s) candidato(s)
      - c) El elector confirma su(s) selección(es)
    - vii. Al confirmar su última elección, la urna imprimirá un testigo de voto.
    - viii. El elector sigue los procedimientos establecidos por el IEC para marcar su credencial para votar.
    - ix. El elector procede a devolver la tarjeta NFC al presidente de casilla, quien le regresará su credencial para votar.
  - c. Cierre.
    - i. El presidente procede a cerrar la urna electrónica de acuerdo a las diferentes razones establecidas por el IEC, llenando o confirmando los datos que la urna electrónica le muestre en pantalla según corresponda.
    - ii. El presidente procede a imprimir un reporte de la votación que mostrará (según los criterios del IEC)
      - a) Folios registrados en la urna electrónica.
      - b) Cantidad de votos para partido político

- c) Cantidad de votos para coalición
- d) Cantidad de votos para candidato(s) independiente(s)
- e) Cantidad de votos para candidatos no registrado(s)
- f) Cantidad de Votos nulos. Si el presidente lo requiere, la urna podrá solicitar la impresión de los folios con las opciones seleccionadas por el elector para verificar la información

g)

d. Algunos ejemplos de casos de uso contemplados

Caso de uso	Resultado
Tarjeta NFC inactiva colocada en la urna electrónica	Urnas no se activa para recibir voto
Tarjeta NFC activa colocada en la urna electrónica y no se retira durante la votación	Urnas se activa para recibir voto, se imprime testigo por cada voto emitido y al terminar de votar el elector la urna desactiva la tarjeta NFC.
Tarjeta NFC activada en urna electrónica de otra casilla	Urnas no se activa para recibir voto
Tarjeta NFC activada en urna electrónica antes de la apertura de la casilla	Urnas no se activa para recibir voto
Tarjeta NFC activa colocada en la urna electrónica y se retira durante la votación	Urnas electrónica se desactivará
Tarjeta NFC activada sustraída de la casilla, clonada n veces y presentada después en la misma casilla para intentar votar	Urnas se activa para recibir el voto por ser un token válido, pero ese token solo funcionará una vez, el resto de las tarjetas NFC no activarán la casilla porque el token ya no es válido.
Tarjeta NFC que se hubiera retirado durante el registro del voto por parte del elector	Urnas electrónica se activará para permitir el voto de los cargos pendientes
Activar 1-n tarjetas NFC	Urnas electrónica se activará en cada caso registrando los votos por cada tarjeta NFC y desactivando cada tarjeta después de cada votación, siempre y cuando los folios se encuentren dentro de los declarados en la apertura de la casilla.

i.

Propuesta Tecnológica

1 Computadora PC compatible LapTop con pantalla touch, 1 Windows 10 Pro, 2 Tarjetas arduino UNO, 2 Lector NFC PN532, Pantalla Oled 0.96" SPI 7P Blanco, mas materiales de instalación para diseño de urna que se monte en una mesa cualquiera.

## Conclusión

La utilización de tarjetas NFC otorga el beneficio de que su contenido puede ser reescrito tantas veces como sea necesario, lo que permitiría a las autoridades electorales eliminar, o disminuir considerablemente, las boletas basadas en papel utilizando desde 1 hasta n tarjetas NFC.

Señales auditivas indicarían que una persona ha concluido su votación, lo que ayudaría a identificar cuando un elector está ocupando una urna innecesariamente después de haber terminado.

Si las autoridades electorales determinaran que es conveniente manejar más tarjetas NFC para agilizar el proceso eso no presenta ningún inconveniente puesto que las terminales lectoras de tarjetas NFC son las responsables de generar el token, el cual debe ser validado por urna electrónica para permitir registrar el voto, y la tarjeta NFC solo transportan información que permiten activar la urna.

Si la tarjeta NFC fuera sustraída de la casilla para ser utilizada en otro lugar, su contenido no sería válido fuera de la misma. porque la urna electrónica valida que el token contenido en la tarjeta NFC pertenezca a esa urna, pudiéndose habilitar una alarma auditiva para identificar el evento de token inválido.

Si la tarjeta NFC fuera sustraída con el propósito de analizar el contenido para reproducir tarjetas NFC válidas, la seguridad de los algoritmos criptográficos actuales ocasionarían que al interesado le tomara tiempos teóricos como los citados en el siguiente ejemplo tomado de [https://www.eetimes.com/document.asp?doc\\_id=1279619#](https://www.eetimes.com/document.asp?doc_id=1279619#):

Tamaño de llave	Tiempo para descifrar el token
128 bit	$1.02 \times 10^{18}$ años
192 bit	$1.872 \times 10^{18}$ años
256 bit	$3.31 \times 10^{56}$ años