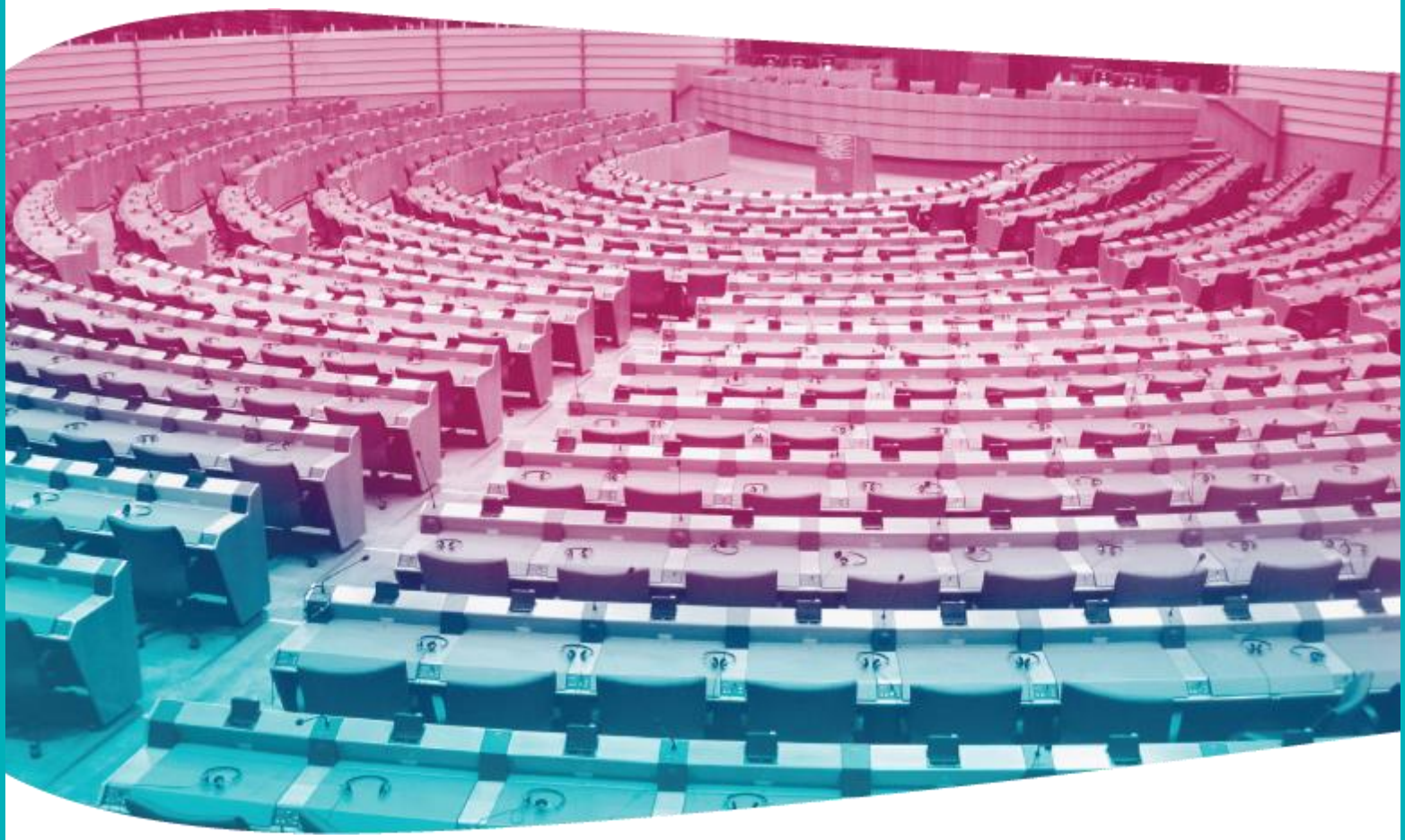
Govlab

Verificación de código de control y recibo – Guía técnica

Versión del software: 14.0.0

Versión del documento: 1.0



Scytl – Election Technologies

STRICTLY CONFIDENTIAL

Tabla de revisiones

Versión	Fecha	Autor	Revisor	Descripción
1.0	23/04/2021	NC		Traducción al español del documento "Control Code and receipt verification"

Tabla de contenidos

Listado de imágenes

01 INTRODUCCIÓN

Este documento tiene como objetivo proporcionar información que permita a cualquier votante validar la integridad y autenticidad de su recibo. Más específicamente, la información proporcionada en este documento debería permitir a los votantes crear una aplicación que valide la firma del recibo utilizando la información proporcionada en el código de control y el recibo en sí.

01.1 Público

El público al que va dirigido de este documento es un ingeniero de software que llevará a cabo la tarea de crear una herramienta que validará el código de control y el recibo.

La comprensión básica de cómo funciona Govlab así como de la criptografía son necesarias para una lectura significativa de este material.

02 VERIFICACIÓN DEL RECIBO Y DEL CÓDIGO DE CONTROL

En esta sección se explica cómo los votantes pueden verificar el recibo, así como el código de control.

02.1 Pre-requisitos

Antes de ir más lejos, es importante entender para qué se usan el recibo y el código de control y cómo se construyen.

Después de que un votante emita su voto, se le proporcionará un recibo y un código de control como los que se muestran en la siguiente imagen:

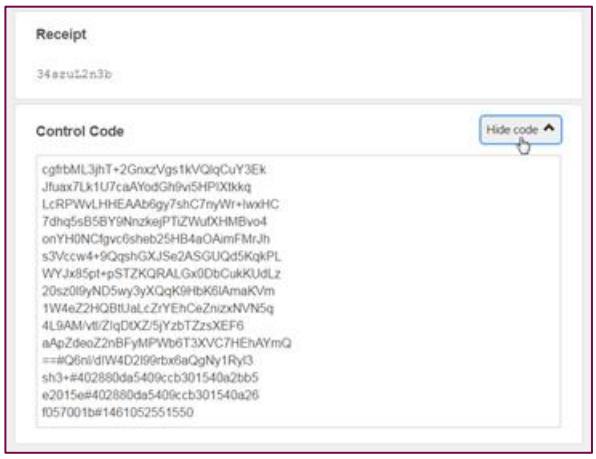


Imagen 1 - Recibo y código de control

El recibo, que se calcula a partir de un valor aleatorio de 192 bits (el *Ballot Identifier*) es utilizado por el votante para confirmar que su voto ha sido correctamente descifrado. Una vez finalizado el proceso de escrutinio, se publica una lista de recibos para que los votantes realicen la verificación. El Código de Control es una firma del recibo que permite verificar su integridad y autenticidad.

Hay varias piezas de información que el votante debe tener antes de validar el código de control y la recepción. A saber:

- El certificado *Message Server X.509 certificate* o la correspondiente clave pública (sólo uno de los dos es necesario).
- El propio Código de Control.

- El propio recibo.

Una vez que estos elementos están disponibles, podemos continuar con los siguientes pasos.

02.1.1 Algoritmos criptográficos

Durante la generación y validación del recibo y el código de control se utilizan los siguientes algoritmos criptográficos.

- Función de hash: SHA256.
- Algoritmo de firma: RSA2048 con SHA256 siguiendo el standard PKCS#1 v1.5.

02.1.2 Estructuras de datos

02.1.2.1 El recibo

El recibo es la representación en base64 del hash del *Ballot Identifier*, truncado a los 10 primeros 10 caracteres.

02.1.2.2 El código de control

El código de control es esencialmente una concatenación de cinco (5) elementos unidos por el carácter almohadilla (#):

- La primera parte es la representación en base64 de la firma de otra concatenación de cuatro (4) elementos unidos por el carácter punto y coma (;):
    - Representación en Base64 del doble hash del *Ballot Identifier.*
    - Identificador de la elección (EID).
    - Identificador de la agrupación de elecciones (EEID).
    - *Timestamp*
- La segunda parte es la representación en base64 del *Ballot Identifier*.
- La tercera parte es el identificador de la elección.
- La cuarta parte es el identificador de la agrupación de elecciones.
- La quinta parte es el *Timestamp*.

02.2 Validaciones

Con el fin de validar la autenticidad y la integridad del recibo, hay dos validaciones que se pueden hacer:

- Confirmación de que el código de control es una firma válida del recibo, realizada por el servidor de votación usando la clave privada *Message Server private key*.
- Confirmación de que los 10 caracteres que se muestran como recibo corresponden al valor firmado por el servidor de votación, cuya firma se ha validado en el paso anterior.

02.2.1 Pasos para validar la firma

Para validar la firma calculada por el servidor de votación, almacenada en la primera parte del código de control, es necesario realizar los pasos siguientes:

1) Extraer las cinco partes del código de control, diviendo la cadena proporcionada usando el carácter almohadilla (#):

```
codigo_de_control[1] = base64_cod(firma)

codigo_de_control[2] = base64_cod(ballotIdentifier)

codigo_de_control[3] = EID

codigo_de_control[4] = EEID

codigo_de_control[5] = timestamp
```

2) Si se ha proporcionado el *Message Server X.509 certificate*, extraer la correspondiente clave pública.
3) Decodificar en base64 el *Ballot Identifier*.

```
ballotIdentifier = base64_decod(codigo_de_control[2])
```

4) Calcular el doble hash del *Ballot Identifier* y codificarlo en base64.

```
base64_cod(hash(hash(ballotIdentifier)))
```

5) Concatenar el valor obtenido en el paso anteriores con el identificador de la elección (EID), el identificador de la agrupación de elecciones (EEID) y el *timestamp*, utilizando el carácter punto y coma (;). Esta es la información firmada por el servidor de votación.

```
infoFirmada =
base64_cod(hash(hash(ballotIdentifier)));codigo_de_control[3];
codigo_de_control[4]; codigo_de_control[5]
```

6) Decodificar en base64 la firma

```
firma = base64_decod(codigo_de_control[1])
```

7) Validar la firma usando la clave pública *Message Server public key*.

```
verif_firma(message_server_pk,firma,infoFirmada)
```

02.2.2 Pasos para validar el recibo

Para validar el recibo es necesario ejecutar los pasos siguientes:

1) Decodificar en base64 el *Ballot Identifier.*

```
ballotIdentifier = base64_decod(control_code[2])
```

2) Calcular el hash del *Ballot Identifier* y codificarlo en base64.

```
base64_cod(hash(ballotIdentifier))
```

3) Comprobar que el recibo proporcionado coincide con los 10 primeros caracteres del valor calculado en el paso anterior.

02.3 Resultado esperado

Si ambas validaciones se realizan correctamente, el proceso debe generar un mensaje de éxito. En cualquier otro caso debe producir un error indicando lo que salió mal. Algunos de estos escenarios de error serían los que se indican a continuación:

- Si falta una o varias de las piezas de información necesarias para realizar las validaciones: certificado o clave pública, recibo o código de control.
- Si cualquier elemento proporcionado no es válido (por ejemplo, si el código de control no tiene la estructura esperada).
- Si alguna de las validaciones falla.