

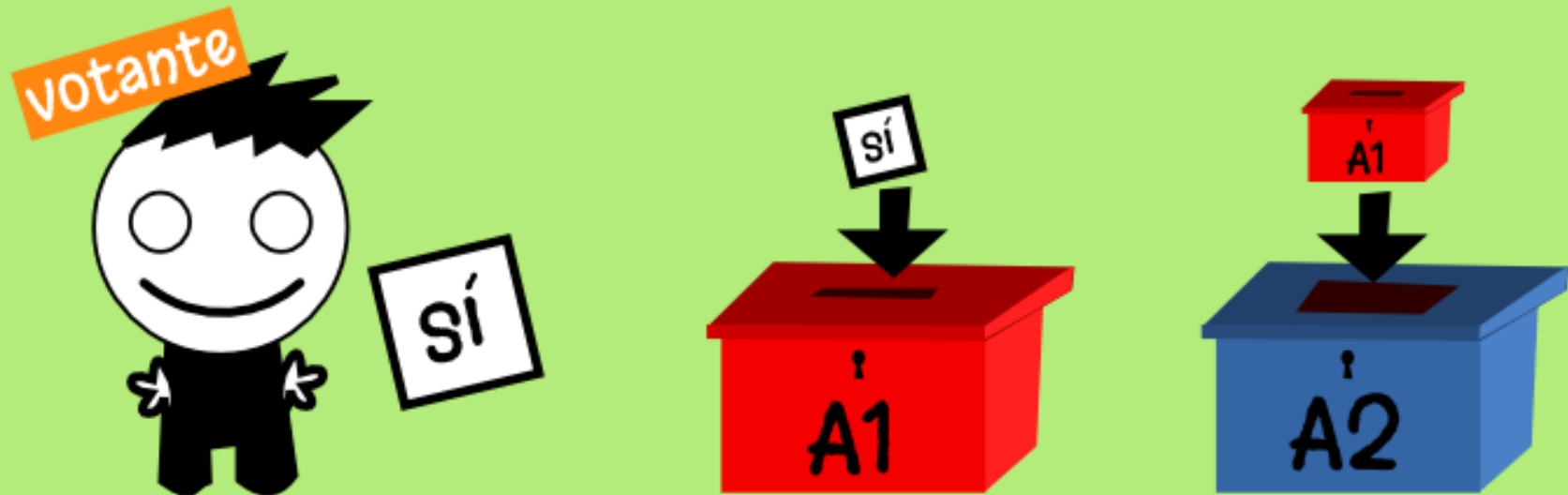
# Agora Voting

Eduardo Robles  
<https://agoravoting.com>  
[edulix@agoravoting.com](mailto:edulix@agoravoting.com)

# Voto electrónico / Voto por internet

# Cómo funciona Agora Voting

# CIFRADO



Cifrado en cliente, el voto no pasa por ningún servidor, todo este proceso ocurre en el ordenador del votante

La caja roja sólo la puede abrir la autoridad A1 y la caja azul sólo la puede abrir la autoridad A2

# HASH DE VOTO

votante



ANTES DE ENVIAR  
MI VOTO VOY A SACARLE  
UNA FOTO Y ME LA GUARDO,  
PARA VERIFICAR EN UN  
FUTURO QUE NADIE LO ALTERE  
Y QUE SE HAYA TENIDO EN  
CUENTA EN EL RECuento



El votante se queda con su hash de voto, que servirá para verificar que su voto se ha tenido en cuenta y que no ha sido alterado. El hash lo genera el propio cliente, por lo que es totalmente confiable.

# ALMACENAMIENTO

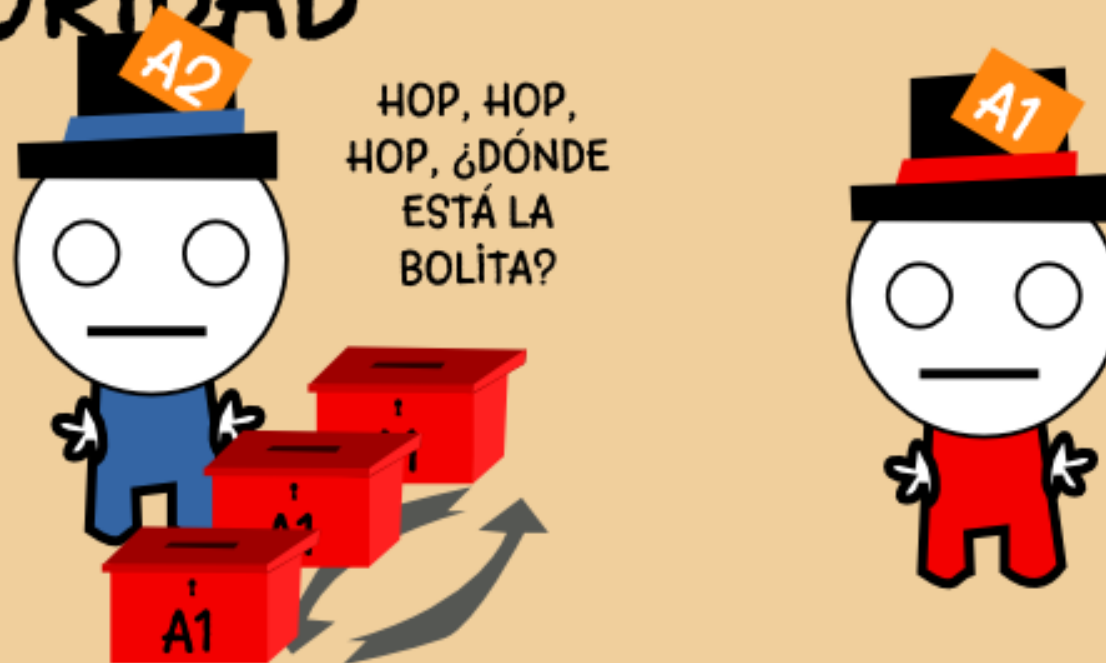


# DESCIFRADO



La autoridad abre las cajas de las que tiene la llave, las azules

# BARAJADO Y PASO A SIGUIENTE AUTORIDAD



La autoridad baraja el resultado antes de pasarselo a la siguiente autoridad



# DESCIFRADO 2



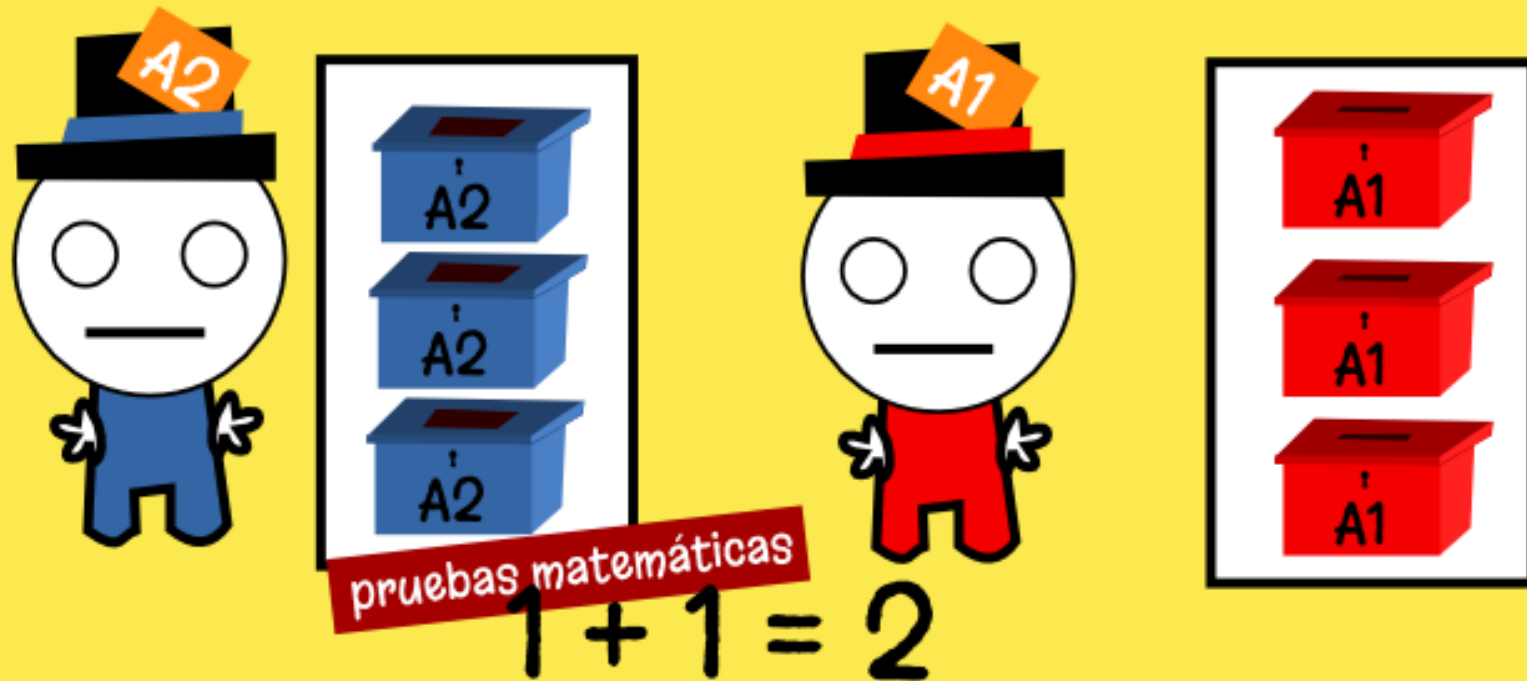
La autoridad abre las cajas de las que tiene la llave, las rojas, y como es la última autoridad obtiene los resultados en claro

# BARAJADO FINAL



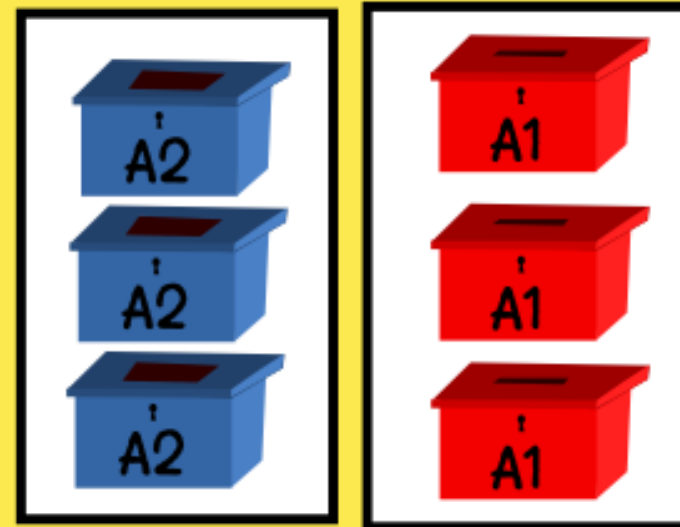
La autoridad baraja el resultado antes de dar el resultado

# VERIFICACIÓN



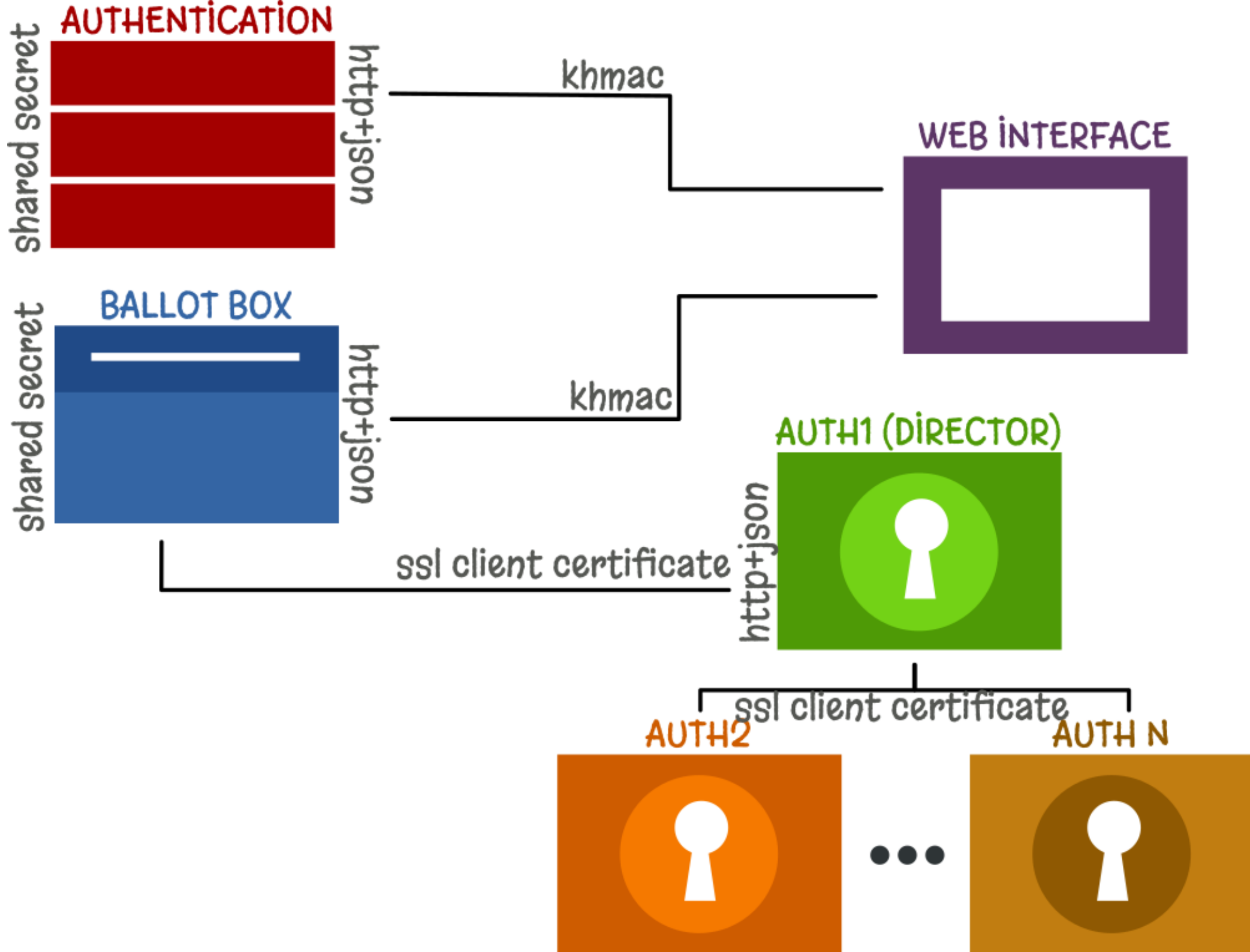
Las autoridades publican las pruebas de que el proceso lo han realizado correctamente para que cualquiera pueda comprobar que no ha habido alteración ninguna en la votación.

# VERIFICACIÓN 2



El votante verifica con su hash que su voto se ha tenido en cuenta y no ha sido alterado

# Arquitectura de AgoraVoting



# AuthApi

# Agora Core View



# Agora Elections

# Autoridades:

- \* Election orchestra
- \* VFork

# Despliegue con Ansible

# Desarrollo abierto