ALFA Group, Valencian Research Institute for Artificial Inteligence, Polytechnic University of Valencia (UPV)

Dispute Resolution and Timeliness in e-voting

Jose Luis Martin-Navarro, Antonio M. Larriba, Damián López

Problem

Verification in e-voting protocols allows voters and the general public to confirm the election and other steps of the protocol. However, it is insufficient to correct the problem, find the culprit or prove it to others.

Definitions

- Disputes: a voter claims that an authority is dishonest while the authority claims to have followed the protocol.
- Dispute resolution: the protocol provides unambiguous evidence in the event of a dispute.
- Timeliness: the voter possess evidence to resolve disputes no later than the election's end.
- Individual Accountability: an attack can be attributed to an entity with public, undeniable evidence.

Protocol

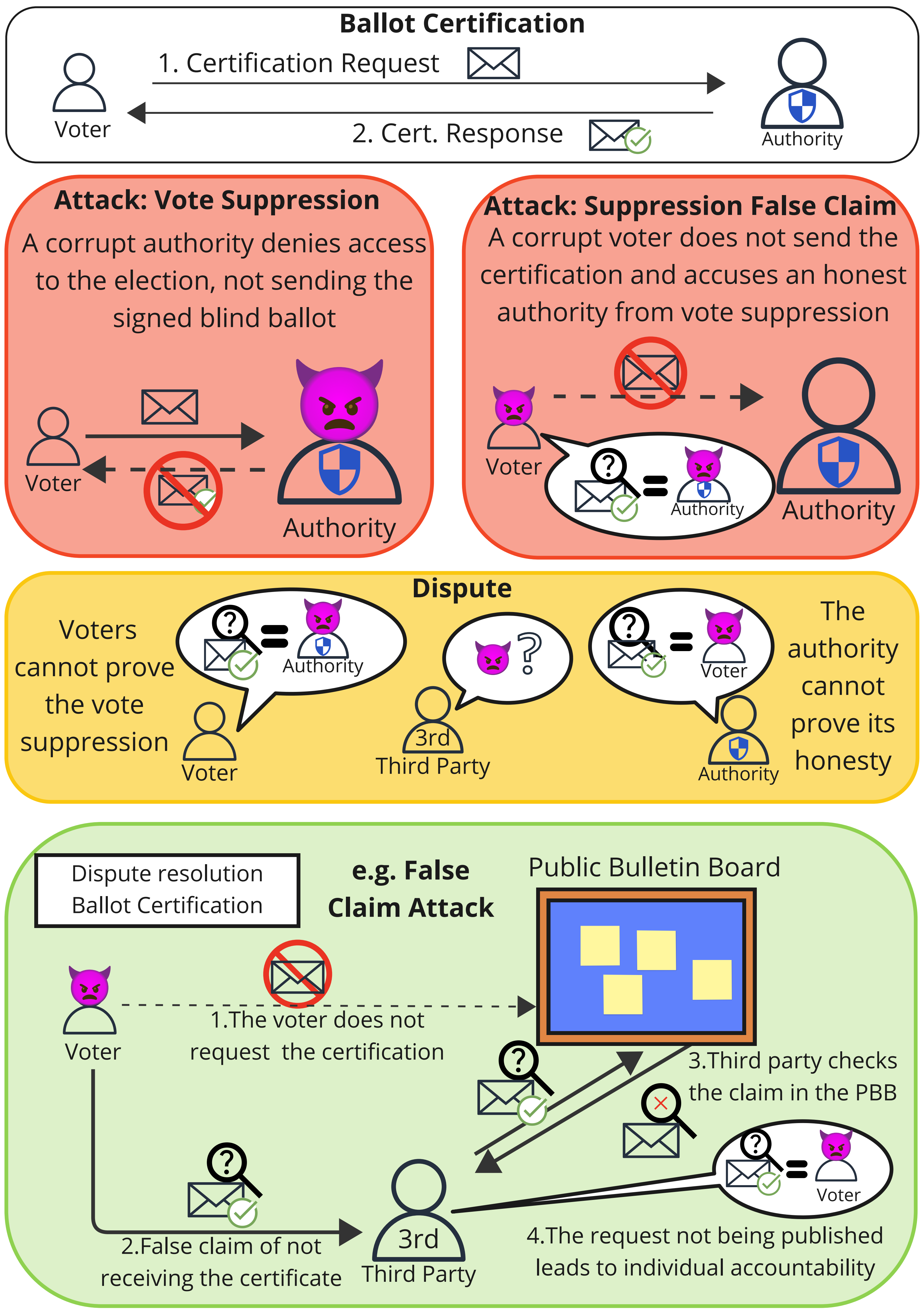
We expand SUVS, an existing multi-tally voting protocol based on blind signatures. The extension includes:

- New dispute about vote suppression:
  - The authority blocks the voter during the ballot certification.
  - Dispute resolution with individual accountability.
- Protection against Denial of Casting:
  - Improved Timeliness: voter can detect issues before the tally.
  - Recovery: voters can use the multiparty tally system to recover from the attack and cast the same ballot.

Future work

- Extend the security analysis with formal verification.
- Secure implementation and proof of concept.

Dispute Resolution & Individual Accountability



Attack: Vote Suppression — A corrupt authority denies access to the election, not sending the signed blind ballot

Attack: Suppression False Claim — A corrupt voter does not send the certification and accuses an honest authority from vote suppression

Voters cannot prove the vote suppression

The authority cannot prove its honesty

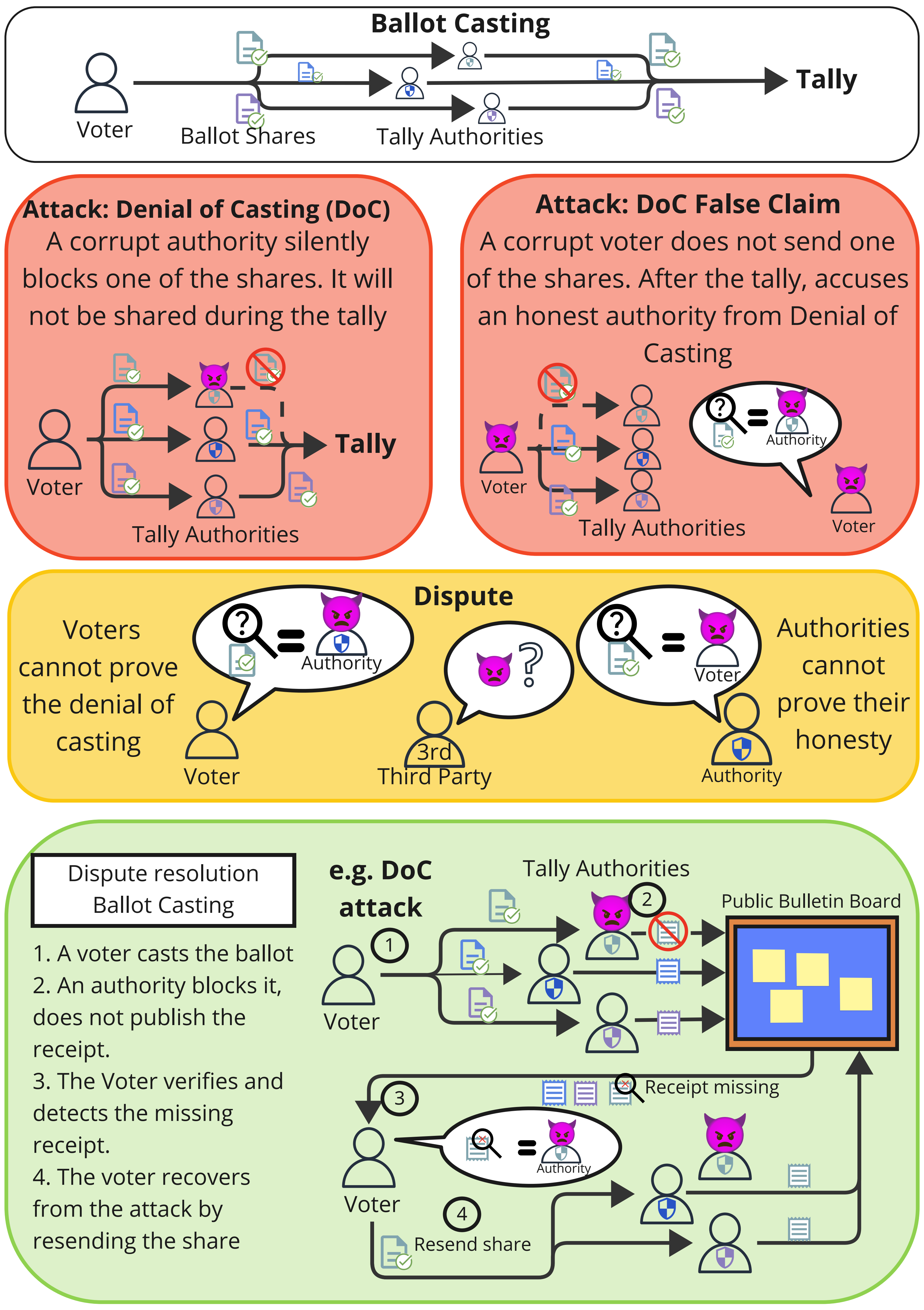
1.The voter does not request the certification

2.False claim of not receiving the certificate

3.Third party checks the claim in the PBB

4.The request not being published leads to individual accountability

Cast Timeliness & Recovery



Attack: Denial of Casting (DoC) — A corrupt authority silently blocks one of the shares. It will not be shared during the tally

Attack: DoC False Claim — A corrupt voter does not send one of the shares. After the tally, accuses an honest authority from Denial of Casting

Voters cannot prove the denial of casting

Authorities cannot prove their honesty

1. A voter casts the ballot
2. An authority blocks it, does not publish the receipt.
3. The Voter verifies and detects the missing receipt.
4. The voter recovers from the attack by resending the share

By INCIBE's Chair, funded by the EU-NextGenerationEU through the Spanish government's Plan de Recuperación, Transformación y Resiliencia. **Contact**: jomarna6@upv.es