Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

Blockchain and eVoting

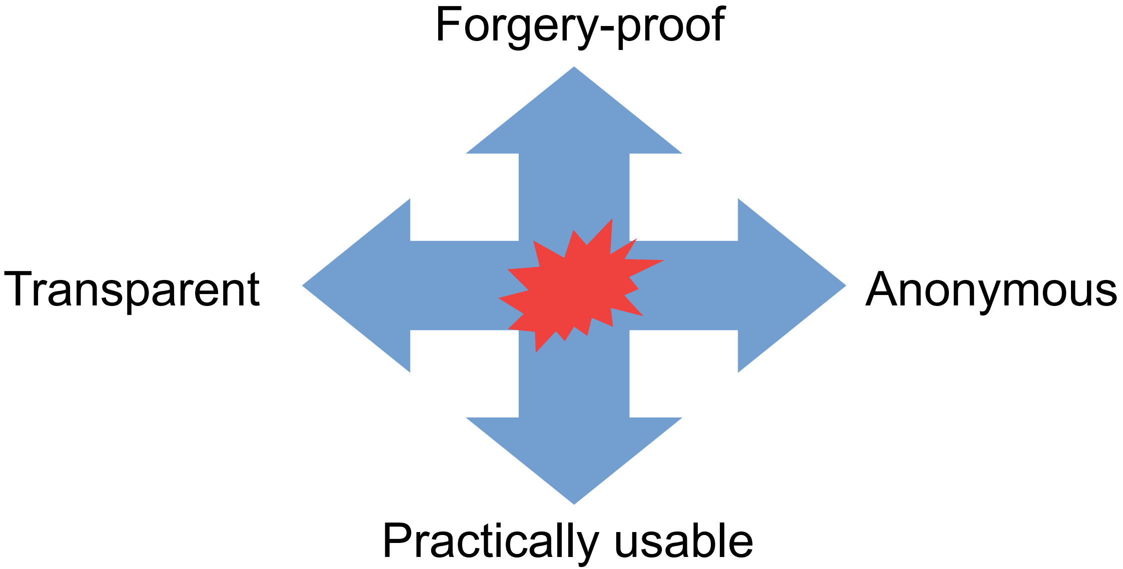
Daniel Peters, PTB
WG 8.52 Embedded Metrological Systems

What is e-Voting?

Electronic voting is an **online** process in which **registered** voters cast their vote from an electronic device and transmit it via the Internet to an electronic ballot box (or **bulletin board**).

Challenge

- **Construct a network in which voters can anonymously change their ballot even after they already cast it, before the deadline passed.**



e-Voting mechanisms

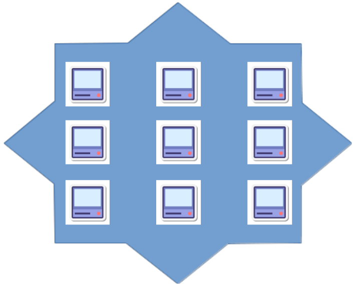
IT mechanisms for secure e-Voting:

- **(Blind) Signatures**
- **Distributed Ledger Technology**
- **Mix Networks (Onion-encryption)**
- **Zero-knowledge Proofs**
- **Identity Based Cryptography**
- **(a)symmetric Encryption**
- **Public Key Infrastructure**
- **Hash functions**
- Homomorphic Encryption Schemes
- Multi-party computations

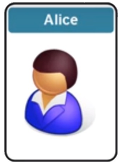
e-Voting Infrastructure

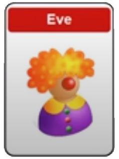
Central Authority

Anonymization Network

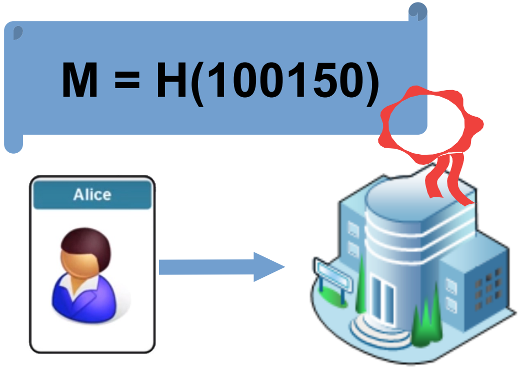


Public Database





Blinded Signatures



Alice wants her m to get signed by CA without disclosing it.

1) Alice uses the publicKey A from CA to transfom the message m to an unreadable form by using a random number k.
2) As a result of mathematically combining m, publicKey A and k she generates an encrypted message m* and sends m* to CA
3) CA deletes Alice out of the list of allowed voters to avoid double votings
4) CA uses m* and its private Key from A to create a signature on m* obtaining s* and sends the message to alice securely
5) Alice uses k to revert her encryption on s* and gets a signature s from CA for m without disclosing m to CA.

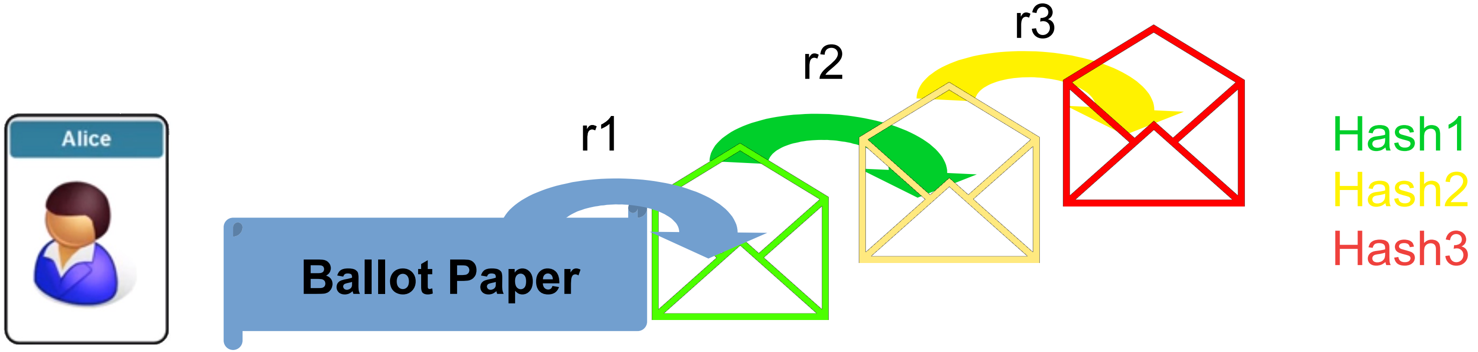
Token System

We make use of two different tokens, called:

1) The Network Usage Token (NUT)
2) The Initial Voting Token (IVT)

- These are all blind signed hashes by the CA
- Voter generates i + b + n different random numbers and their hashes.
- CA generates a new key pair (pk_NUT , sk_NUT) for every time slot

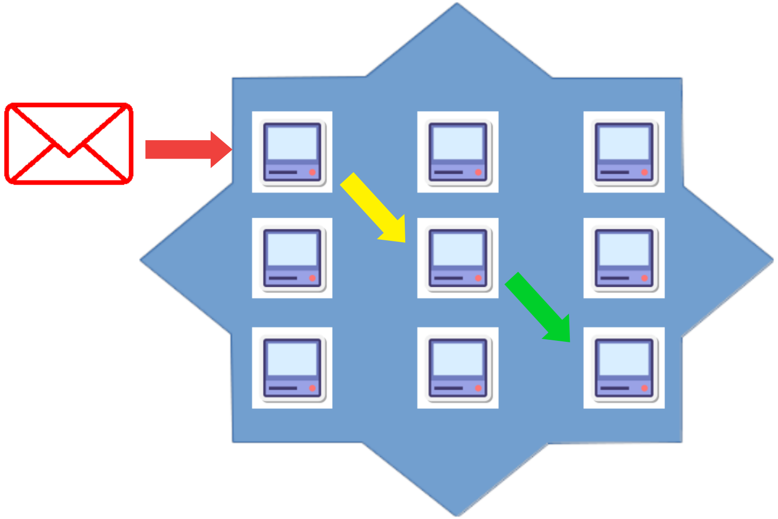
Ballot onion encryption



1. Alice uses the public key of node1 to encrypt her Ballot and a random number (r1) choosen by Alice (green envelope)
2. She creates a hash value of „green envelope“ and saves it together with r1
3. Alice uses public key of node 2 to package the „green envelope“ in yellow one adding another random number and noticing the hash of „yellow envelope“
4. She does the same for the red envelope using node 3 public key

To open an envelope the corresponding node private key is needed, which is only known to the node itself

Ballot onion decryption



Every step is snchronized by the CA by defining time slots

1)MixServer1 notices the „yellow envelope“ on the public database

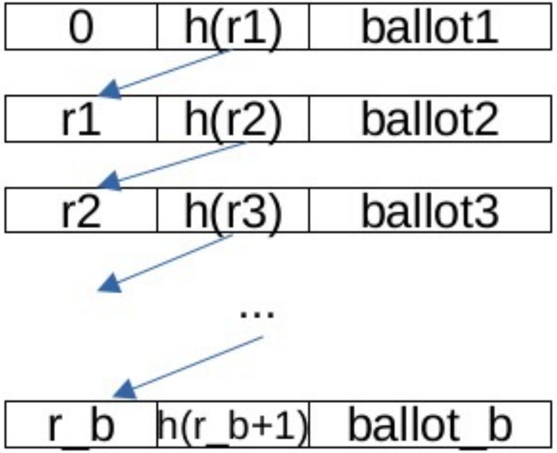
2)MixServer1 extracts the „yellow envelope“ and writes the „green envelope“ to the database

3)MixServer 1 generates a zkProof to show that mixing is correct

4)MixServer2 does the same ...

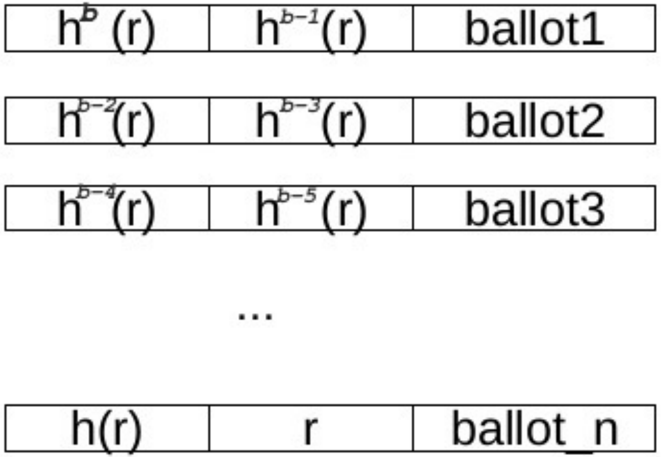
Re-Voting

IVT signed



0	h(r1)	ballot1
r1	h(r2)	ballot2
r2	h(r3)	ballot3
...		
r_b	h(r_b+1)	ballot_b

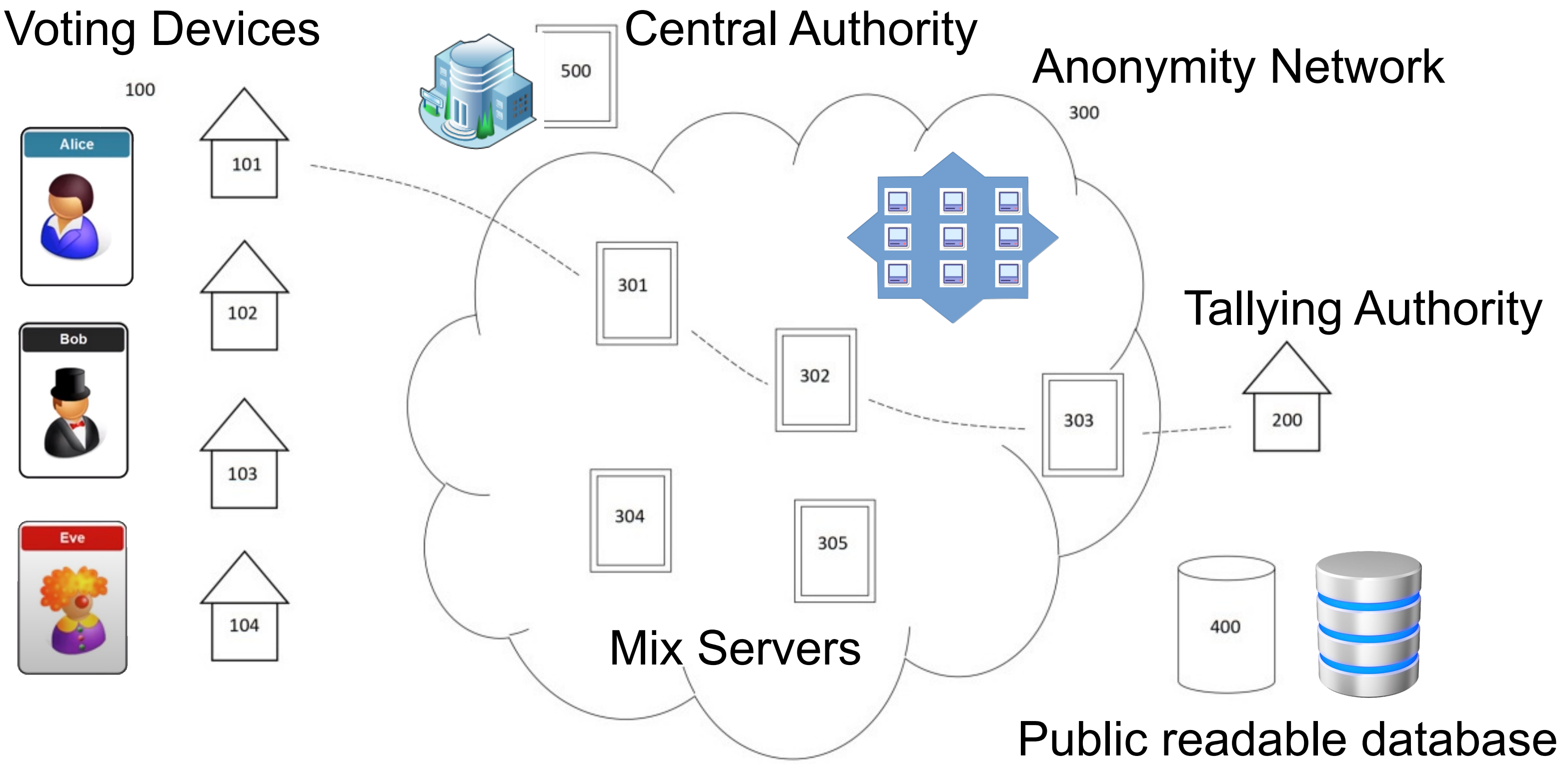
IVT signed



$h^{b}(r)$	$h^{b-1}(r)$	ballot1
$h^{b-2}(r)$	$h^{b-3}(r)$	ballot2
$h^{b-4}(r)$	$h^{b-5}(r)$	ballot3
...		
h(r)	r	ballot_n

Ballots before union encryption

Our network topology



Central Authority

- Is accessible all the time
- Checks if voters are permitted to vote
- Generates blind signatures for IVT and NUT
- Synchronizes the anonymity network
- Verifies the zkProofs

Anonymity Network

- The MixNet is synchronized by the CA and every stepped is logged
- The synchronization takes place by using time-frames
- Logged in a public readable database which is permissioned
- Only the CA has write-access to it

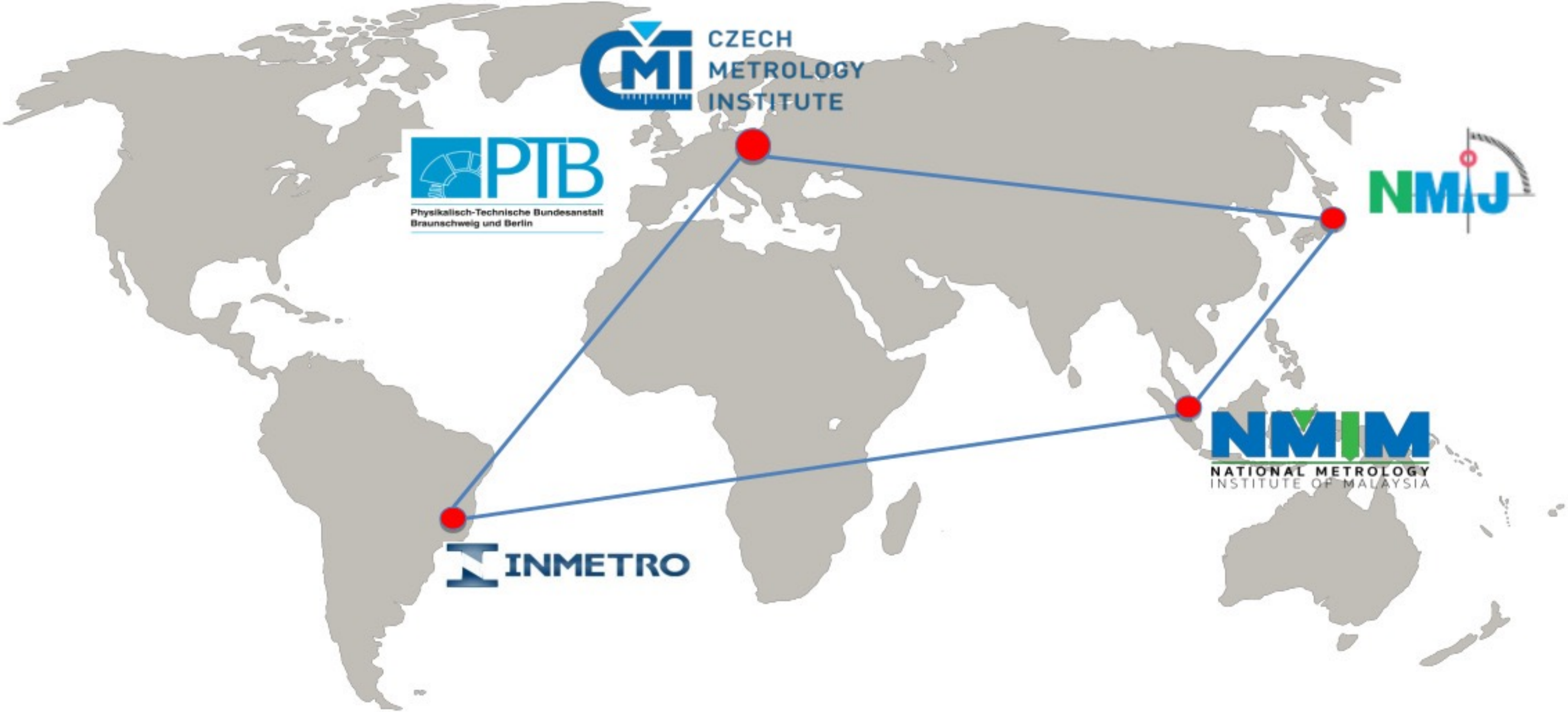
Voting Application

- An easy to use graphical user interface
- The blind signature implementation, for the communication with the CA
- Secure random number creation
- ID checking on the device
- Communication with the anonymity network
- Choosing the order of the MixServers, through which the ballot should be onion-encrypted and sent

Overall Procedure / Conclusion

1) The tallying authority starts a new election through the CA
2) A voter identifies herself to the CA, and the CA gives authorization through blind signed tokens
3) The voter uses the anonymity network to submit her onion-encrypted vote. She authorizes herself for using the anonymity network through the signed NUT
4) The nodes in the anonymity network send all their batches of votes that they received in a time slot mixed with a zkProof to the CA. The CA checks the NUT tokens (from the entry MixServers) and the zkProofs for every step.
5) The CA puts the next layer of encryption onto the public database for the next MixServer
6) This is repeated until only the completely decrypted ballot paper is left
7) Because of the hash properties, voters can change their mind by sending new ballots that are linked with the old ones before the deadline has passed.

Real Research Network


CZECH METROLOGY INSTITUTE
PTB
Physikalisch-Technische Bundesanstalt Braunschweig und Berlin
NMIJ
NMIM
NATIONAL METROLOGY INSTITUTE OF MALAYSIA
INMETRO

Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Abbestrasse 2-12
10587 Berlin

Dr. Daniel Peters
Telefon: 030 3481-7916
E-Mail: daniel.peters@ptb.de
www.ptb.de