Scytl
Innovating Democracy

Yellow in motion. SWISS POST

CYBER ATTACKS AND DEFENSE
SWISS CYBER STORM
WWW.SWISSCYBERSTORM.COM

SwissPost/Scytl

Online Voting Solution

Swiss Cyber Storm 2017

October 2017

SwissPost/Scytl

Experince in Switzerland

Presence in Switzerland since the beginning

2000 Ordinance from the Federal Council allowing online voting pilots

2004 Neuchâtel deploys online voting system from Scytl with advanced security: e2e encryption, anonymous decryption (Mixnet) and voter verifiability (receipts)

2014 Ordinance from Federal Council establishing new security requirements (inspired by Scytl's online voting solution in Norway), so that cantons can expand online voting to 30, 50 and 100% of their voting population

2015 Neuchâtel implements individual verifiability with Scytl system and received new 30% authorization level.

2015 Scytl enters into a partnership with SwissPost and join develop a voting system

2015 Zurich Consortium did not pass the authorization process

2016 Fribourg adopts SwissPost/Scytl online voting system 30% authorization level

2016 Neuchâtel migrates to SwissPost/Scytl online voting system

2017 Bassel-Stadt and Thurgau adopts SwissPost/Scytl voting system

2017 SwissPost/Scytl online voting system receives 50% certification level

Individual Verifiable Voting Solution

Certified with 50% level

Protocol design principles

- Authenticity:
  - Individual voter digital signatures (key roaming)
- Privacy:
  - e2e encryption
  - Anonymous decryption (Mix-net)
  - Secret sharing schemes
- Integrity:
  - Digital signature of votes and election information
- No coercion / vote buying
  - Voters cannot completely prove their intention to third parties
- Auditability and Verifiability
  - Individual verifiable for voters using Return Codes and voting receipts
  - Universal verifiable for anybody using a universal verifiable Mixnet and digital signatures
  - Immutable logs based on cryptographic chaining information (private blockchain)
  - Provable secure through cryptographic and formal proves

Voting Process

Individual Verifiability

The voter receives a verification card by postal mail

Start Voting Key:
A2B5-44F0-92BB-23DC-1234

Return Codes:
Answer A – 4523
Answer B – 0423
Answer C – 2412
…

Ballot Casting Key – 1452 32
Vote Cast Code – 1245 1003

unique for each voter

Scytl
Innovating Democracy
SWISS POST

Voting phase

Authenticating

Start Voting Key:
A2B5-44F0-92BB-23DC-1234

Return Codes:

Answer A	–	4523
Answer B	–	0423
Answer C	–	2412

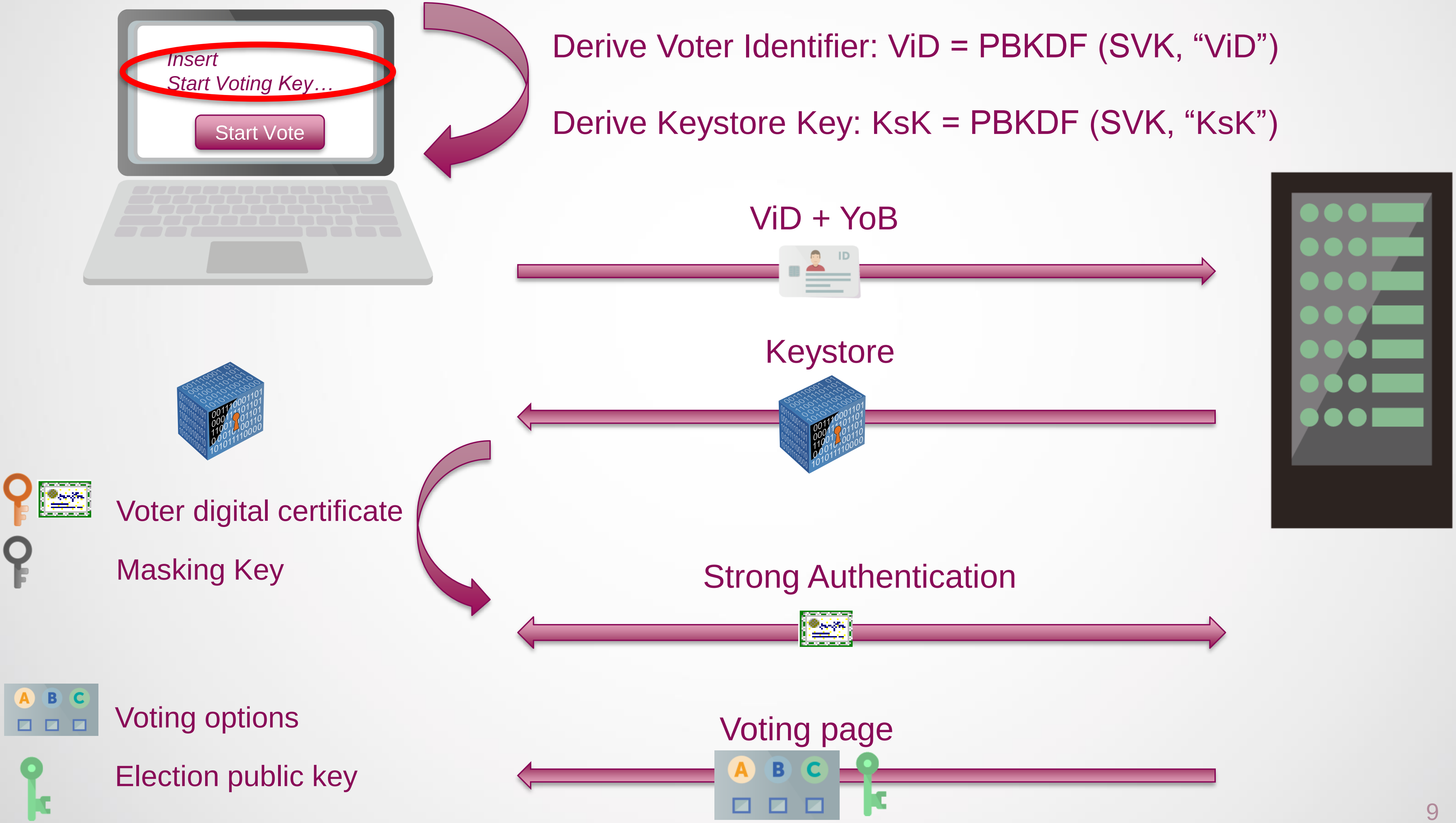
Ballot Casting Key – 1452 3241

Vote Cast Code – 1245 1003

Insert Start Voting Key
Insert Year of Birth

Voting phase

Authentication



Derive Voter Identifier: ViD = PBKDF (SVK, “ViD”)

Derive Keystore Key: KsK = PBKDF (SVK, “KsK”)

ViD + YoB

Keystore

Voter digital certificate

Masking Key

Strong Authentication

Voting options

Election public key

Voting page

Voting phase

Selecting voting options

Start Voting Key:
A2B5-44F0-92BB-23DC-1234

Return Codes:

Answer A	–	4523
Answer B	–	0423
Answer C	–	2412

Ballot Casting Key – 1452 3241

Vote Cast Code – 1245 1003

Voting phase

Sending the vote

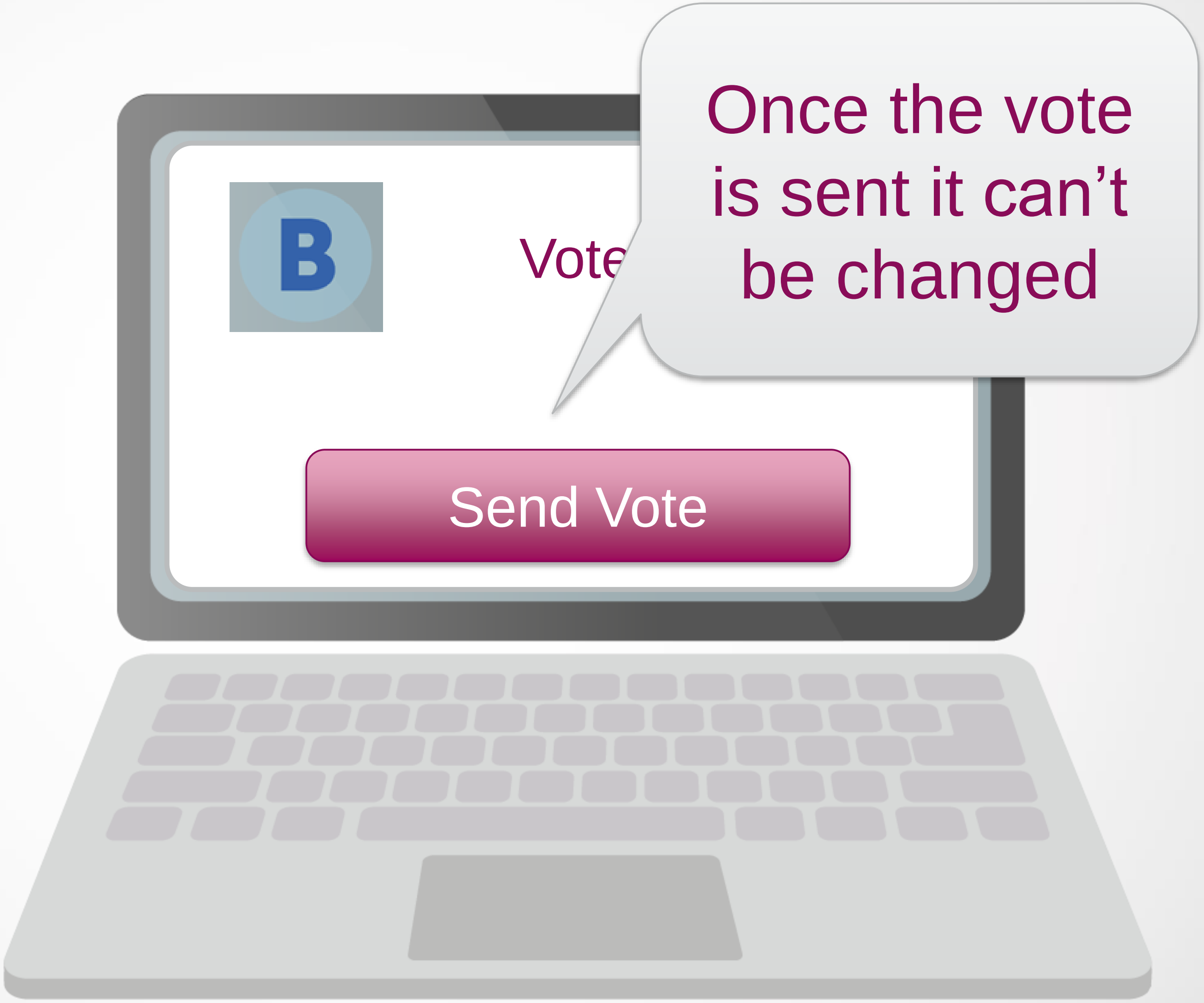
Start Voting Key:
A2B5-44F0-92BB-23DC-1234

Return Codes:

Answer A	–	4523
Answer B	–	0423
Answer C	–	2412

Ballot Casting Key – 1452 3241

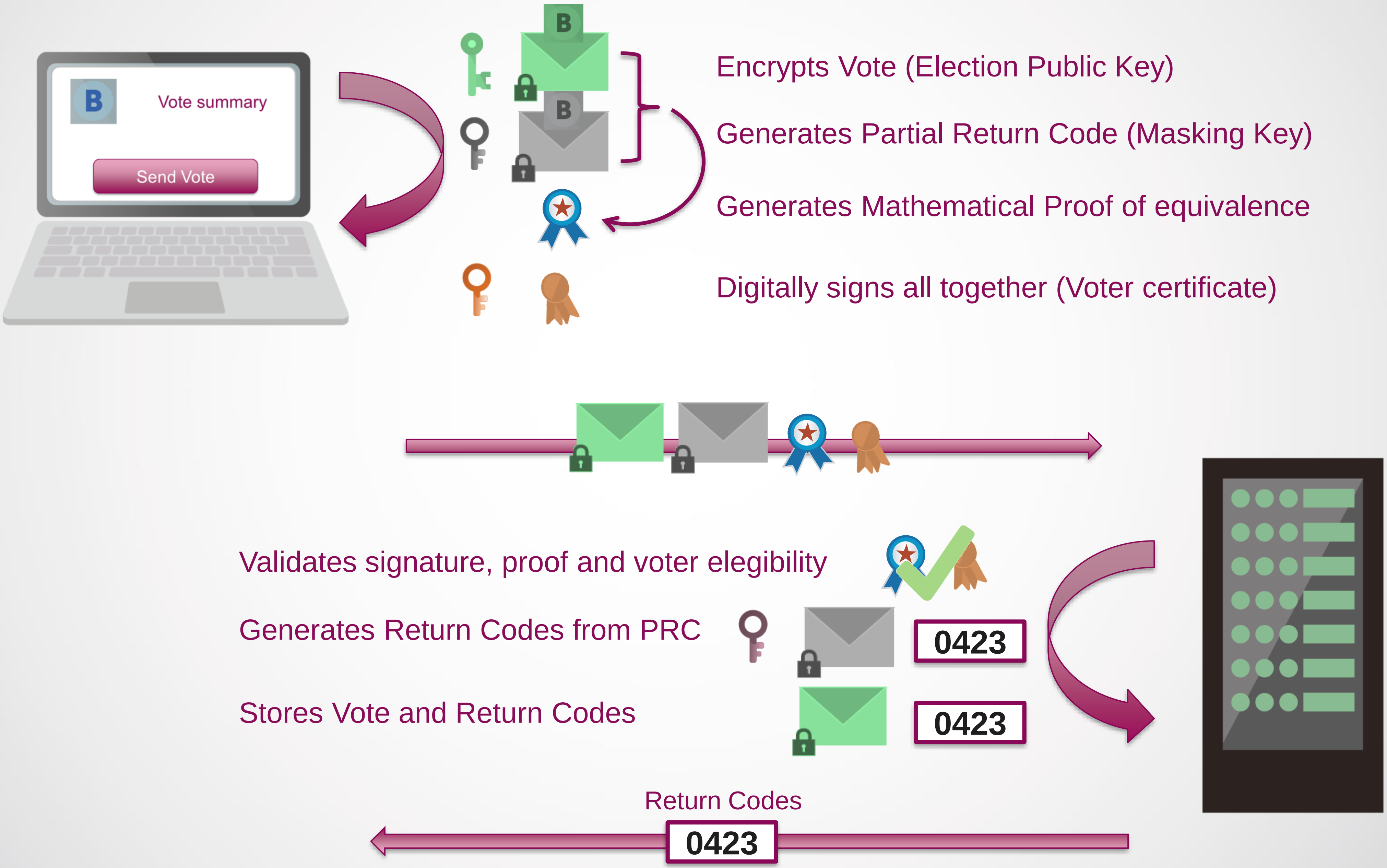
Vote Cast Code – 1245 1003



Once the vote is sent it can’t be changed

Voting phase

Authentication



Encrypts Vote (Election Public Key)

Generates Partial Return Code (Masking Key)

Generates Mathematical Proof of equivalence

Digitally signs all together (Voter certificate)

Validates signature, proof and voter elegibility

Generates Return Codes from PRC

Stores Vote and Return Codes

Return Codes

0423

Innovating Democracy

Voting phase

Verifying return codes

Start Voting Key:
A2B5-44F0-92BB-23DC-1234

Return Codes:

Answer A	–	4523
Answer B	–	0423
Answer C	–	2412

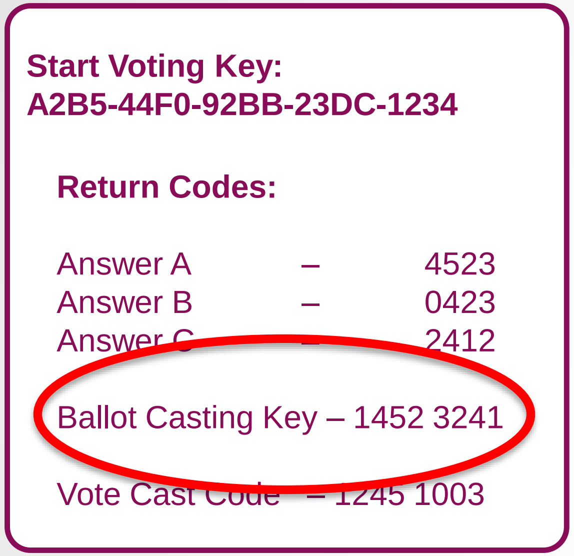
Ballot Casting Key – 1452 3241

Vote Cast Code – 1245 1003

0423
Verify your Return Codes

Voting phase

Confirming the vote



Start Voting Key:
A2B5-44F0-92BB-23DC-1234

Return Codes:

Answer A	–	4523
Answer B	–	0423
Answer C	–	2412

Ballot Casting Key – 1452 3241

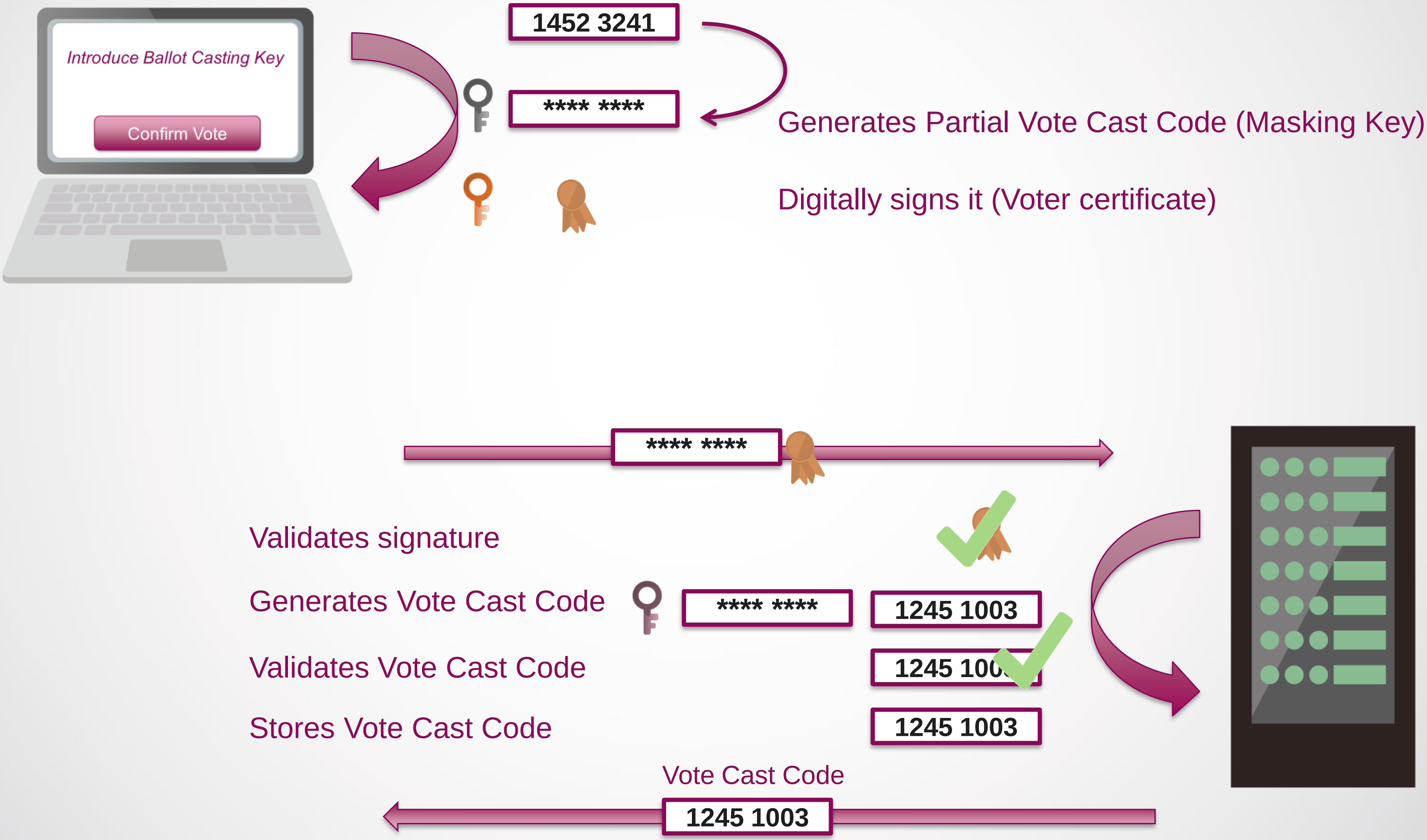
Vote Cast Code – 1245 1003

Introduce Ballot
Confirm Vote

Once the vote is confirmed the voter can’t vote later on by traditional ways

Voting phase

Authentication



Generates Partial Vote Cast Code (Masking Key)

Digitally signs it (Voter certificate)

Validates signature

Generates Vote Cast Code

Validates Vote Cast Code

Stores Vote Cast Code

Vote Cast Code

Voting phase

Verifying the vote casting

Start Voting Key:
A2B5-44F0-92BB-23DC-1234

Return Codes:

Answer A	–	4523
Answer B	–	0423
Answer C	–	2412

Ballot Casting Key 1452 3241

Vote Cast Code – 1245 1003

Verify the Vote Cast Code

1245 1003

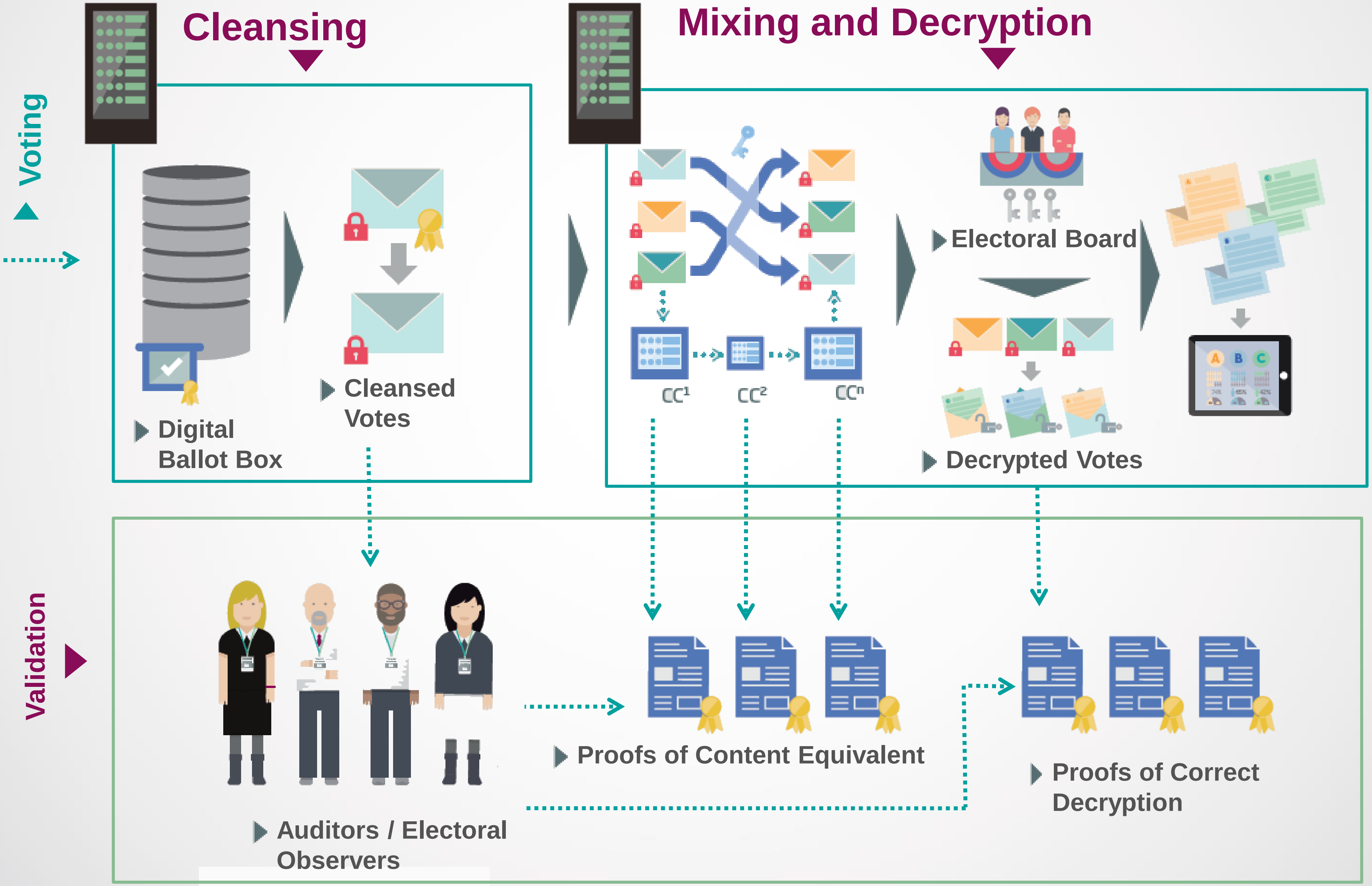
If ok, your vote has been cast!

Counting Phase

Counted as Cast verifiability

Counting Phase

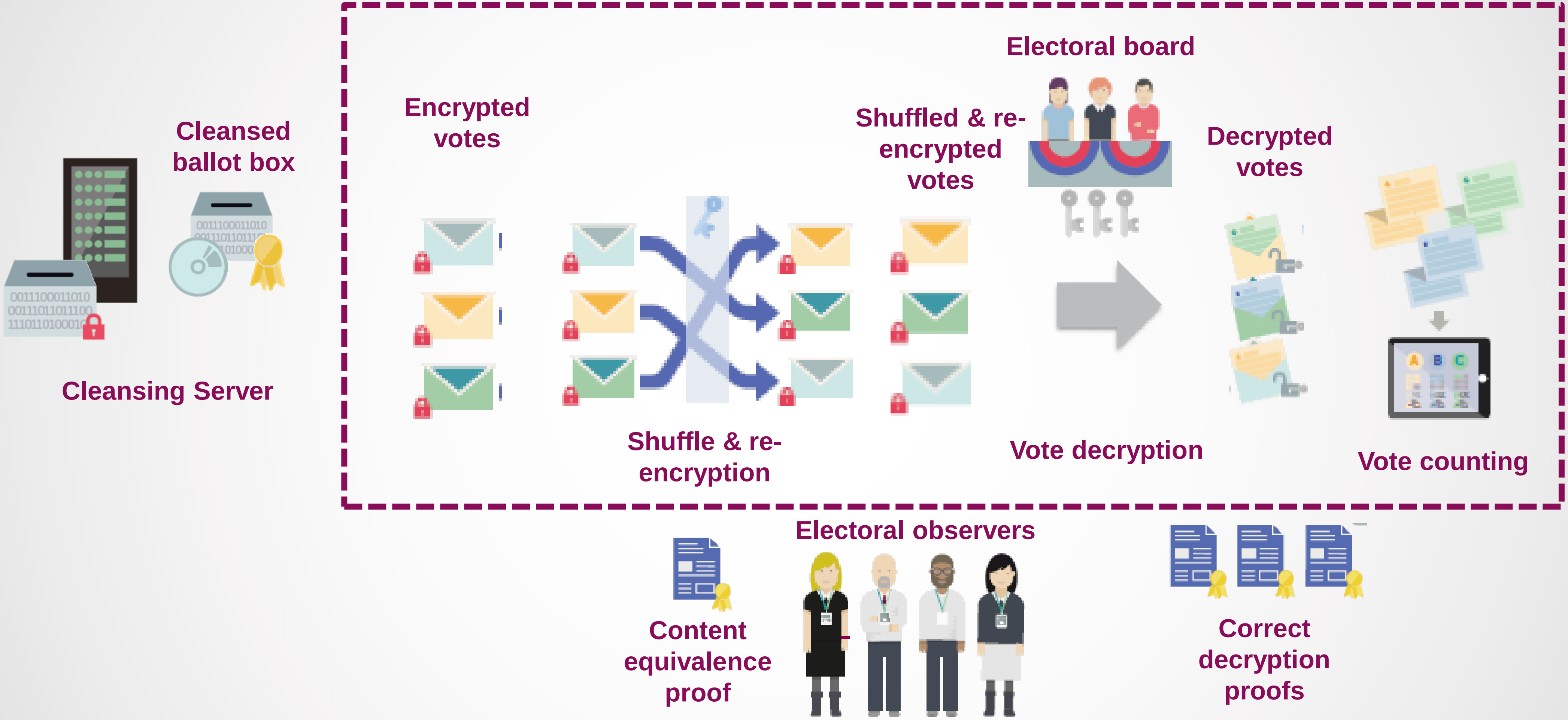
Overview



Mixing and Decryption

Counting Phase

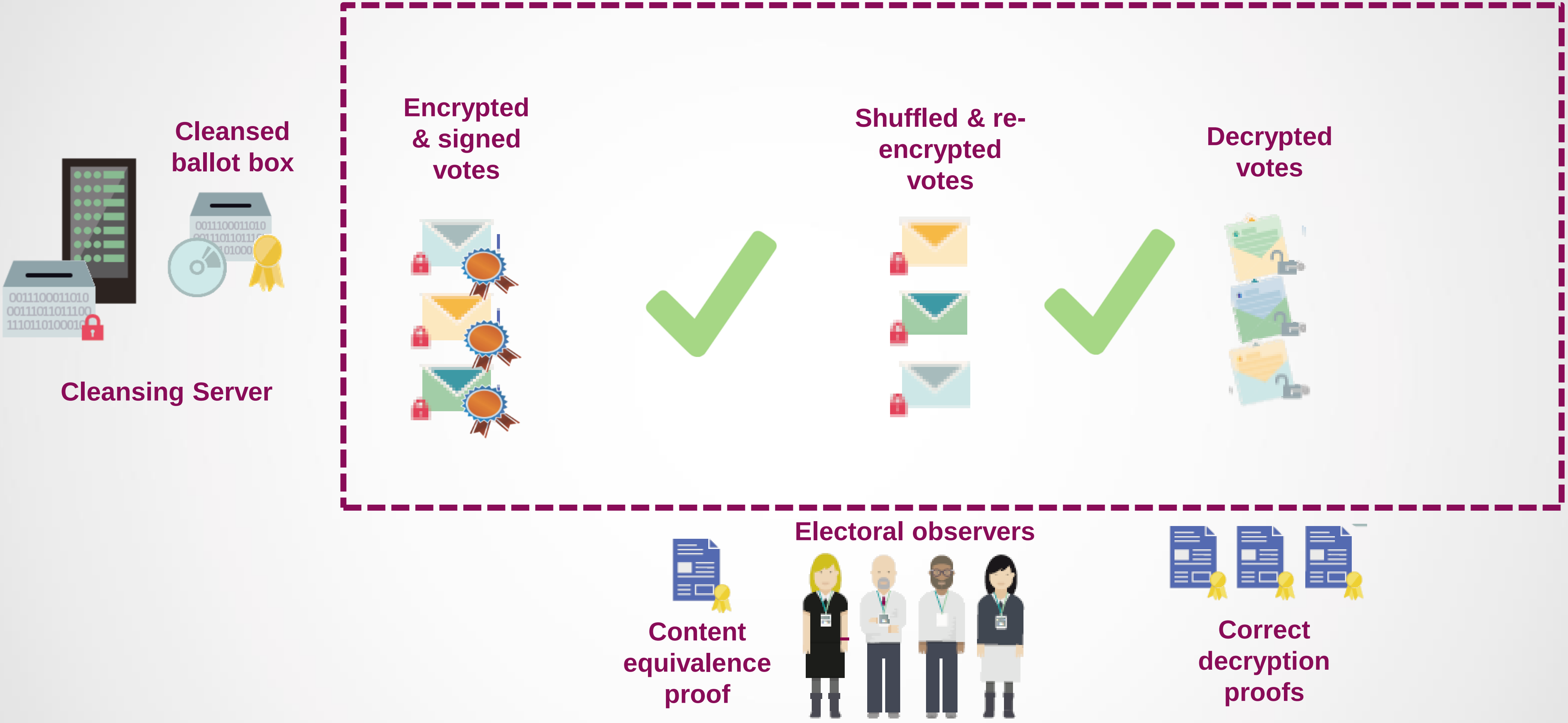
Mixing and Decryption



- ***Proof of content equivalence***: proves that the votes have not been manipulated by the Mixing process. Base on Bayer-Groth proofs.
- ***Proofs of correct decryption***: proves that the votes have not been manipulated during the decryption process

Counting Phase

Counted as cast verifiability



Cleansed ballot box

Cleansing Server

Encrypted & signed votes

Shuffled & re-encrypted votes

Decrypted votes

Electoral observers

Content equivalence proof

Correct decryption proofs

Individual Verifiability Certification

50% Certification Requirements

Security requirements (on top of 30% req.)		Scytl/SwissPost
Common Criteria Framework	Assurance Level 2 (EAL2)	Yes
Individual verifiability	Cast-as-intended functionality	Yes
	Provable secure (cryptographic and formal proofs of the protocol)	Yes

Additional Security properties (not required for 50% level.)		Scytl/SwissPost
E2E encryption	Encryption in the same voter terminal with Election Public key	Yes
Universal verifiable Mixnet	Cryptographic provable proofs of the correct shuffling and decryption	Yes
Vote correctness	Allows to detect invalid votes without compromising voter	Yes
Voting receipts	Voters can check the presence of their vote in counting process	Yes (option)

Scytl
Innovating Democracy

SWISS POST

Complete Verifiable Voting Solution

100% level certification

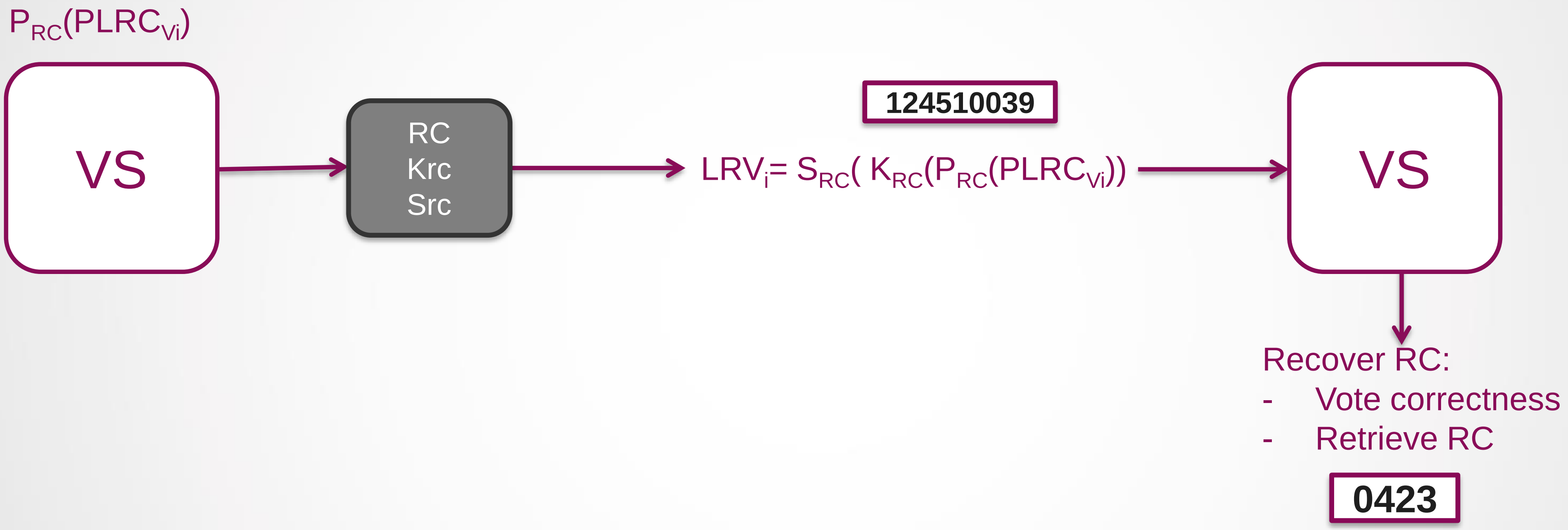
What is a control component?

- Control components can be:
  - A group of people.
  - Computers: at least 4 components per group with different OS.
  - HSMs (EAL4 or FIPS 140-2 level 3 certified): at least 2 components per group from different manufacturers (same OS).
- Components are combined in one or few groups.
- A single component is assumed to be untrustworthy, but at least one per group is assumed to be trustworthy.

ALL THE CONTROL COMPONENTS IN A GROUP HAVE TO COLLABORATE.

Return Codes Generation

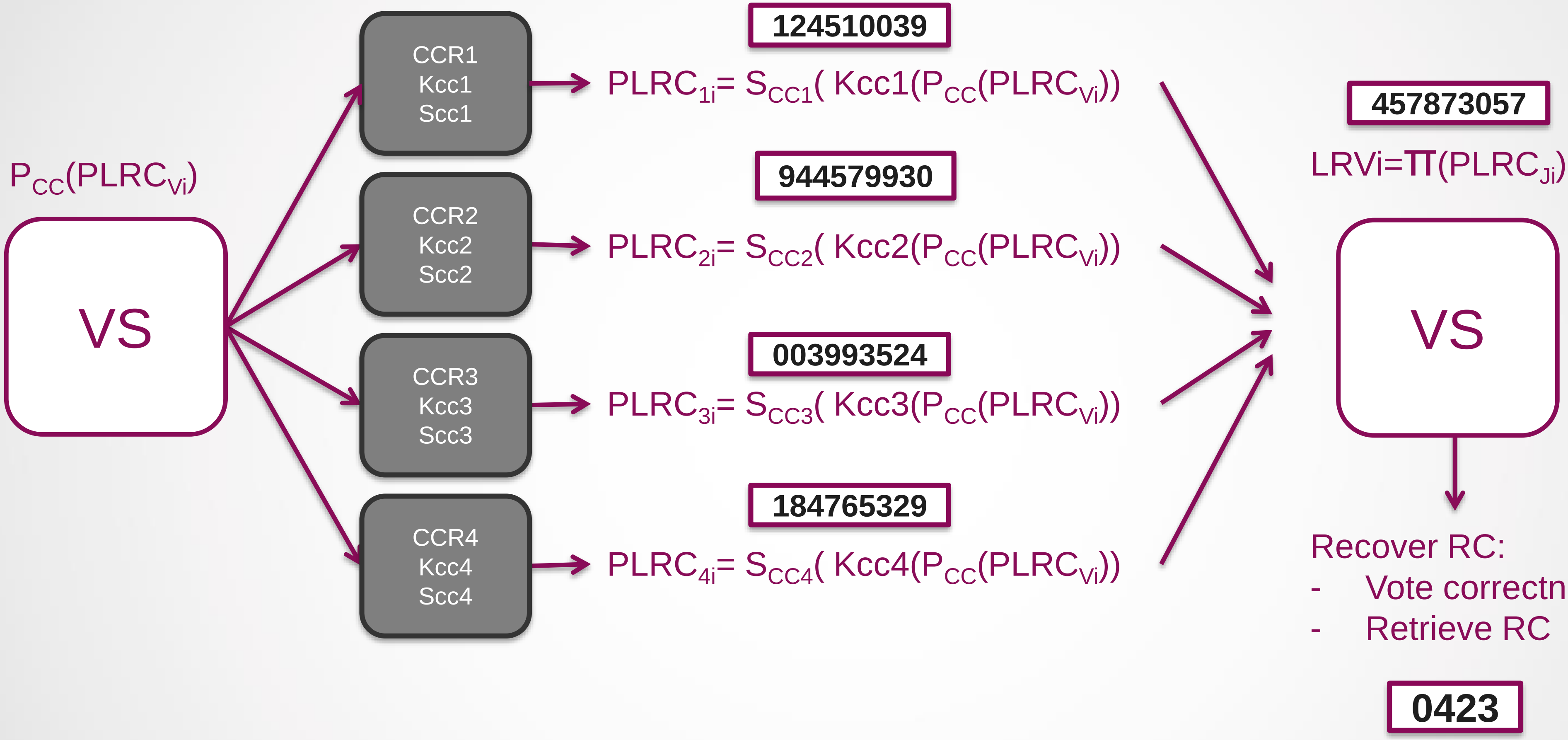
Currently



- Return Code Generator service (RC) operates the encrypted voting options and send the result (LRV) to the voting system (VS)
- Voting System verifies the correntness of the LRV code received and retrieves the final Return Code (RC)

Return Codes Generation

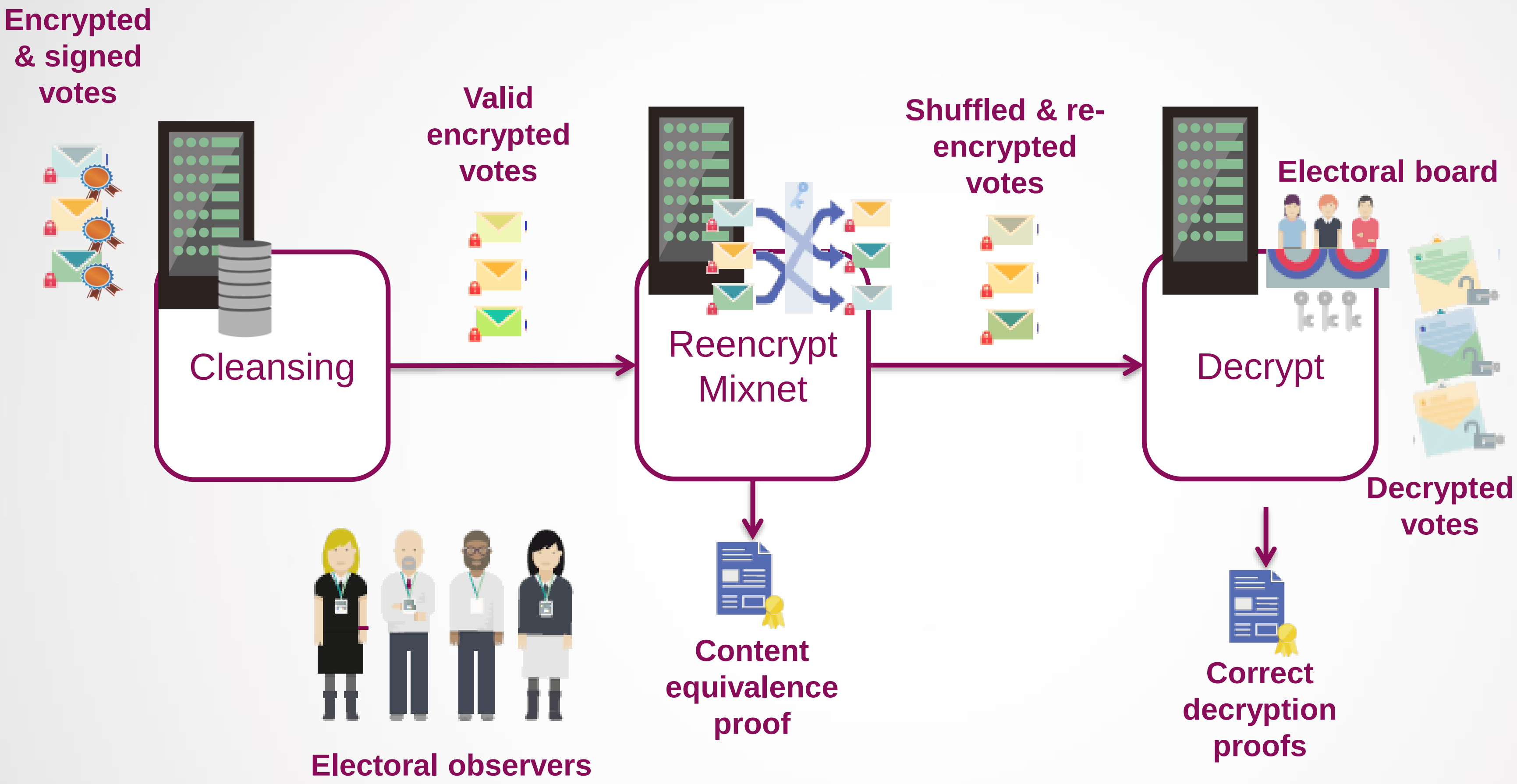
With Control Components



- The original Return Code Generation service is decoupled in 4 independent Return Code Control Components
- Each Control Component has its own key and work in parallel over the encrypted voting options
- Voting system verifies the outputs from the Control Components and combines them to find the Return Code

Mixing and Decrytion

Currently



Encrypted & signed votes

Valid encrypted votes

Shuffled & re-encrypted votes

Electoral board

Cleansing

Reencrypt Mixnet

Decrypt

Decrypted votes

Electoral observers

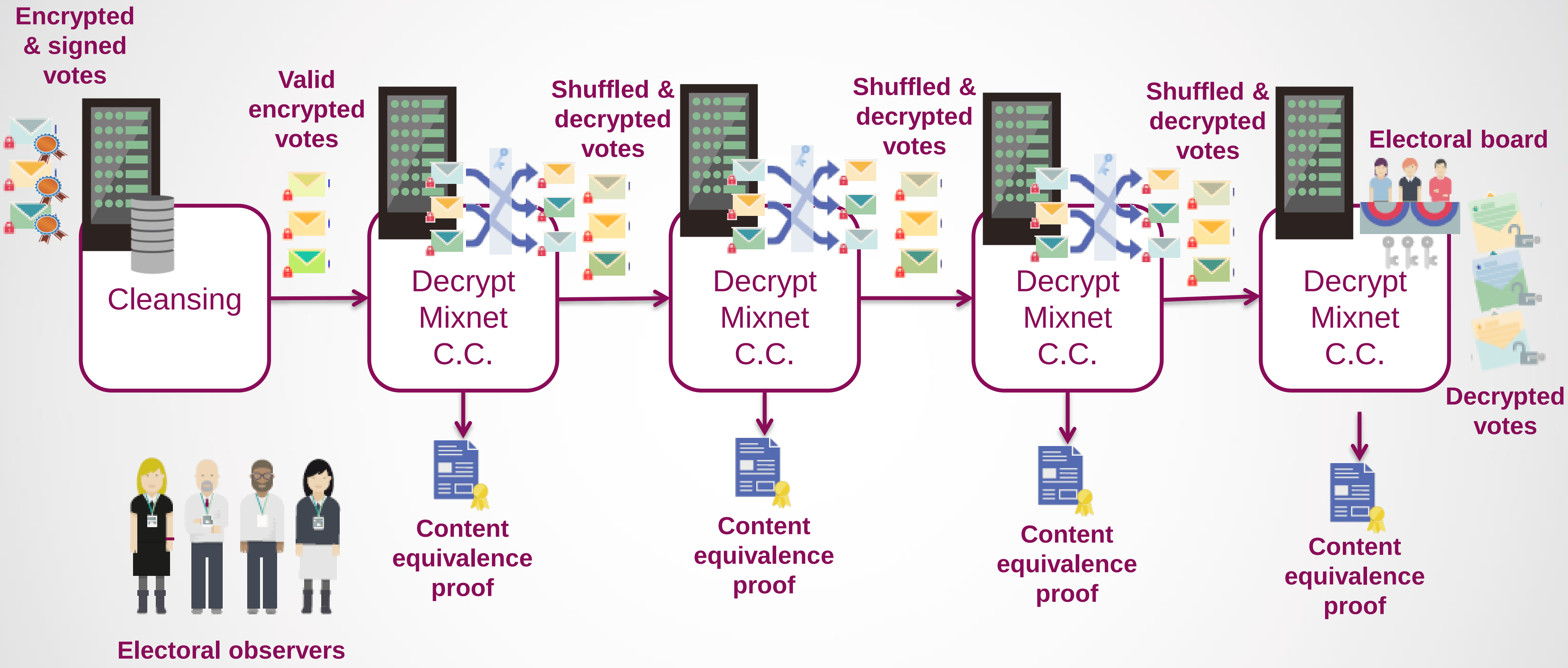
Content equivalence proof

Correct decryption proofs

- Cleansing, Mixing and decryption are done on different machines

Mixing and Decrytion

Control Components



- Cleansing, Mixing and decryption are done by for Control Components

Conclusions

Protocol properties

- Authenticity:
  - Individual voter digital signatures
- Privacy:
  - e2e encryption
  - Anonymous decryption (Mix-net)
  - Secret sharing
- Integrity:
  - digital signature of votes and election information
- No coercion / vote buying
  - Voters cannot completely prove their intention to third parties
- Auditability and Verifiability
  - Individual for voters using Return Codes and voting receipts
  - Universal for anybody using a universal verifiable Mixnet and digital signature
  - Immutable logs based on cryptographic chaining information (private blockchain)
  - Provable secure through cryptographic and formal proves
  - Certified for 50% level and in process for 100% level

Scytl

Innovating Democracy

Yellow in motion. SWISS POST

CYBER ATTACKS AND DEFENSE • SWISS CYBER STORM • WWW.SWISSCYBERSTORM.COM

THANK YOU!

More information and demo.

https://www.post.ch/en/business/a-z-of-subjects/industry-solutions/swiss-post-e-voting

About Scytl:

https://www.scytl.com