EDU-VOTING

Leyla TEKİN[1], Hüseyin Güven ÖZGÜR[2], Burcu Sayın[3], Arzum KARATAŞ[4], Pelin ŞENKULA[5], Emre IRTEM[6], and
Serap ŞAHİN[7]
[1]Izmir Institute of Technology, İzmir/Turkey, leylatekin@iyte.edu.tr
[2]Izmir Institute of Technology, İzmir/Turkey, huseyinozgur@iyte.edu.tr
[3]Izmir Institute of Technology, İzmir/Turkey, burcusayin@iyte.edu.tr
[4]Izmir Institute of Technology, İzmir/Turkey, arzumkaratas@iyte.edu.tr
[5]Izmir Institute of Technology, İzmir/Turkey, pelinsenkula@iyte.edu.tr
[6]Izmir Institute of Technology, İzmir/Turkey, emreirtem@iyte.edu.tr
[7]Izmir Institute of Technology, İzmir/Turkey, serapsahin@iyte.edu.tr

EDU-VOTING: An Educational Homomorphic e-Voting System

Because of the advanced technology, e-voting becomes a hot topic.

Especially, small organizations prefer to use e-voting systems because of its practicability.

There are some security requirements that should be concerned and satisfied.

This study has an educational intuition that analyzes those requirements.

Requirements of an e-voting system

i. Inalterability: Once a vote is casted, it cannot be modified
ii. Non-reusability: A voter must have only one valid vote
iii. Eligibility: Only eligible voters should cast a vote
iv. Fairness: Unless the voting process ends, counting process cannot be started
v. Individual verifiability: Every voter should keep track of whether her own casted vote still in the system or not
vi. Universal verifiability: Everyone can verify the correctness of the whole voting process and results according to announced system keys and data

Requirements of an e-voting system (cont.)

vii. Privacy: Votes cannot be correlated with voters with the help of vote anonymization

viii. Authentication/Identification: Checking the credentials of anyone to see whether the proffered identity consistent or not

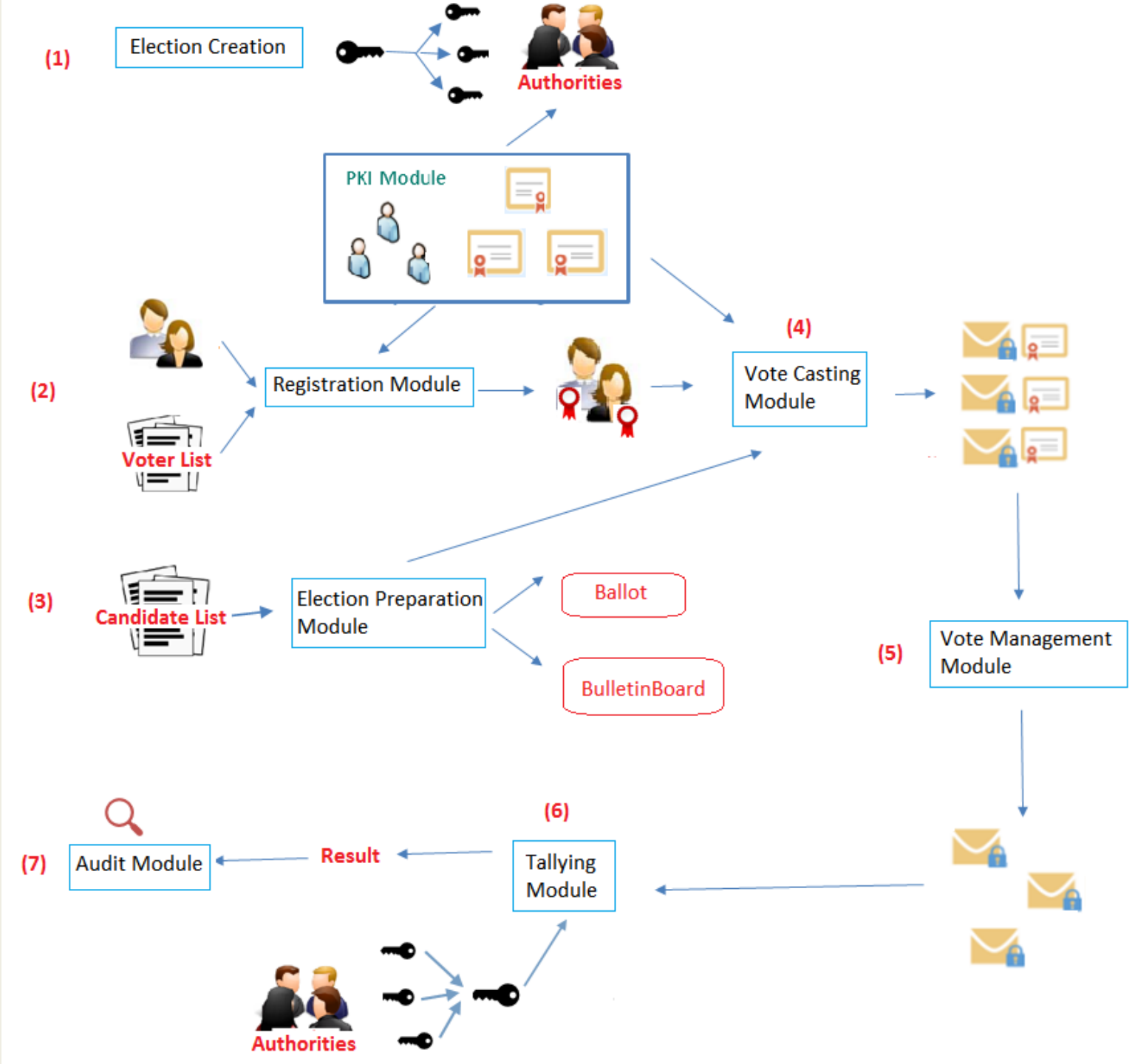
ix. Integrity: While applying some operations on data, protecting the accuracy and consistency of it

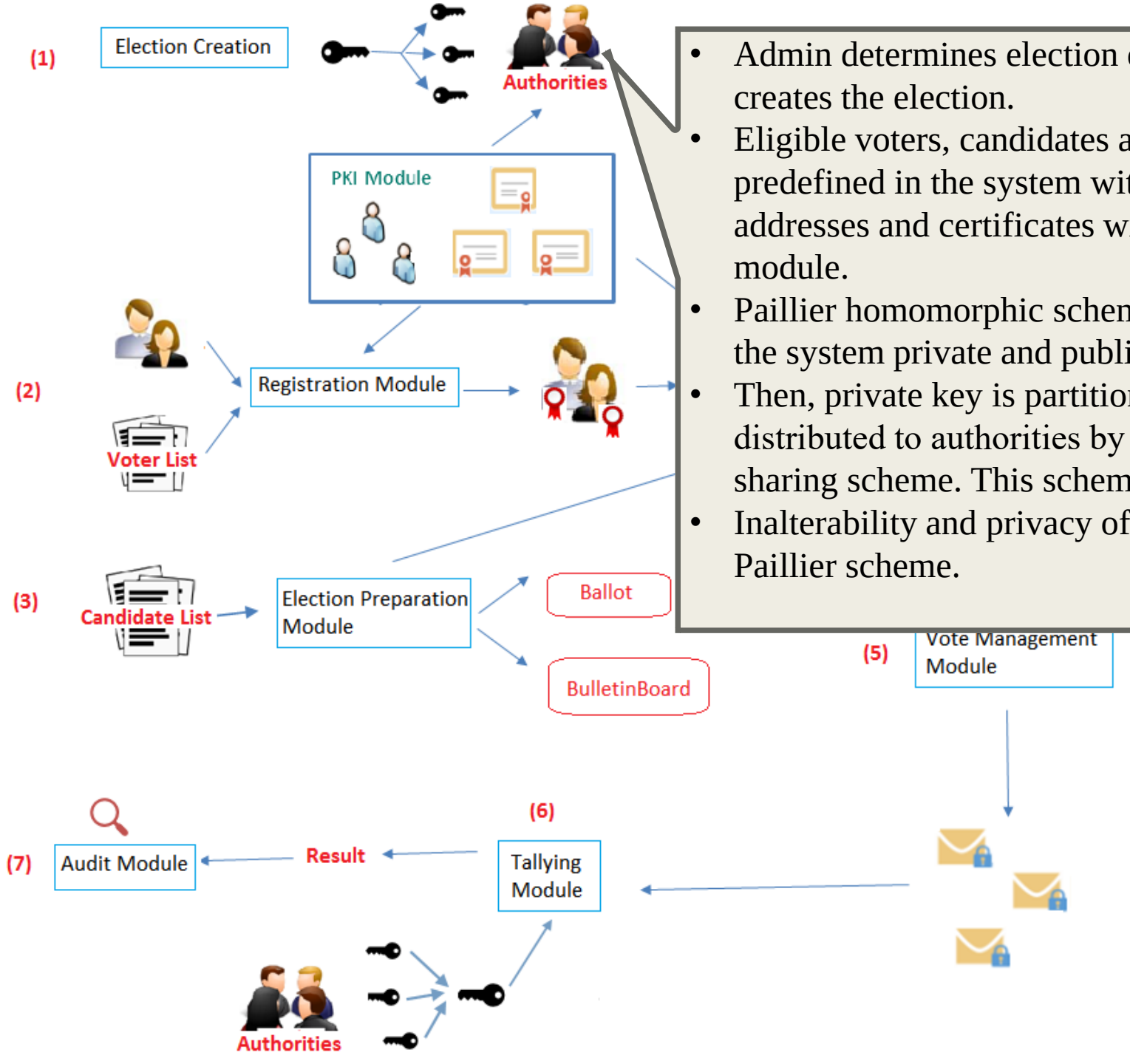
x. Coercion-resistance: Providing a fake credential for every voter to use in any possible coercion case

xi. Receipt-freeness: Attackers cannot find any receipt of a voter's casted vote

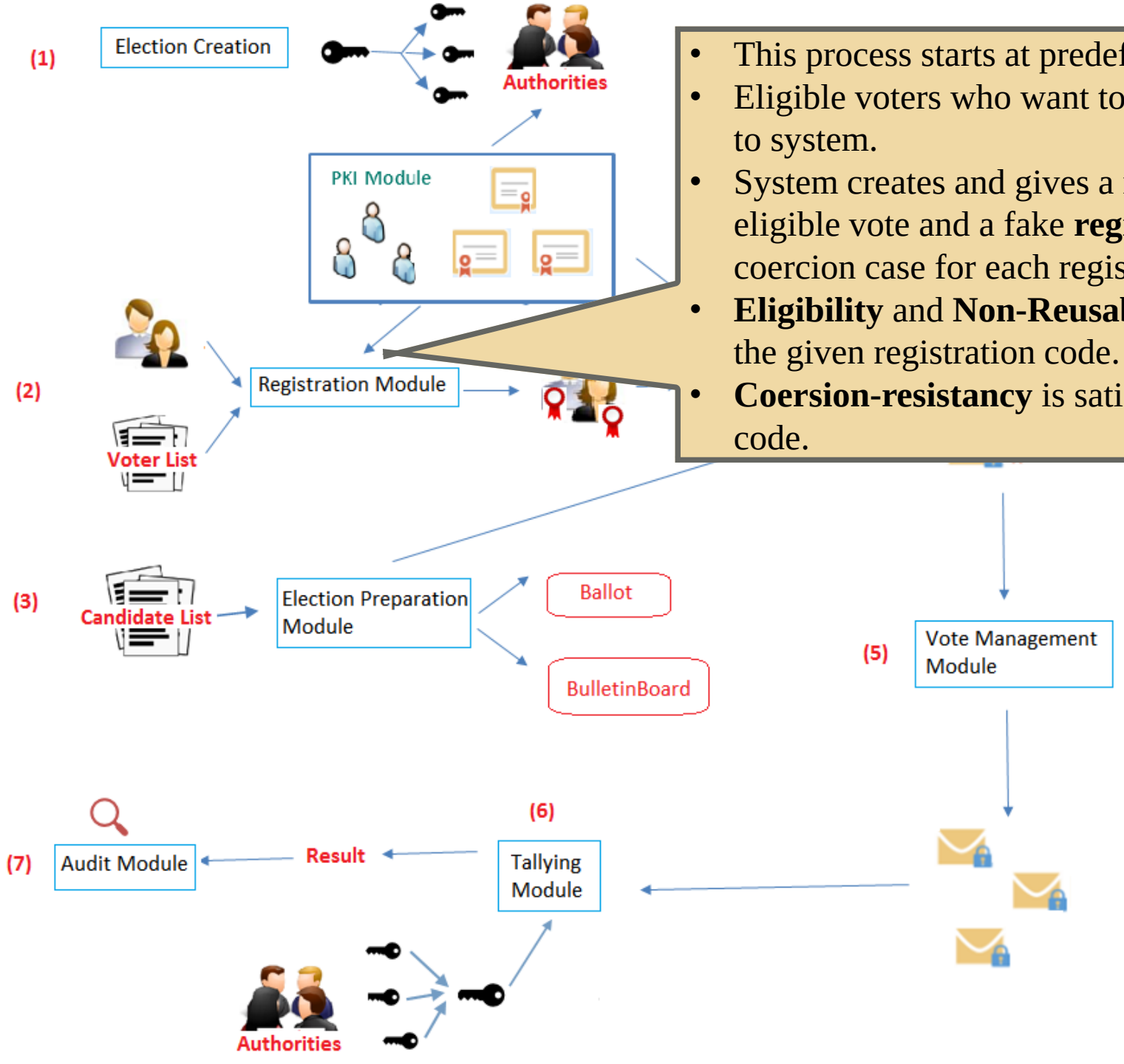
xii. Secrecy: Ensuring that no one can read the message except the intended receiver

In order to build a well-designed e-voting system, key requirements mentioned above should be satisfied.

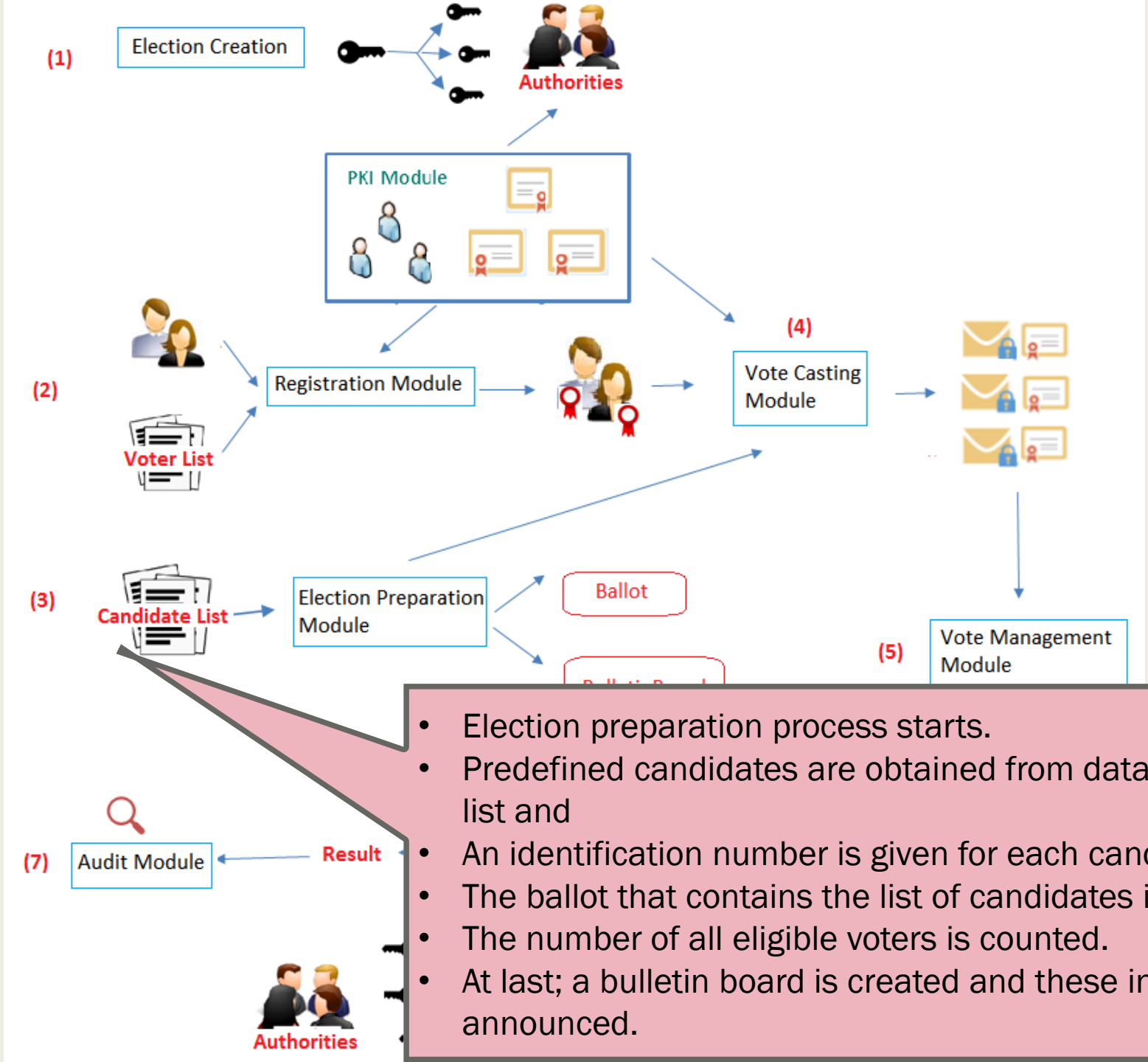

(1)
Election Creation
Authorities
PKI Module
(2)
Registration Module
Voter List
(4)
Vote Casting Module
(3)
Candidate List
Election Preparation Module
Ballot
BulletinBoard
(5)
Vote Management Module
(6)
Tallying Module
(7)
Audit Module
Result
Authorities



- Admin determines election dates and name, then creates the election.
- Eligible voters, candidates and authorities are predefined in the system with their names and email addresses and certificates with the help of PKI module.
- Paillier homomorphic scheme is used to construct the system private and public key.
- Then, private key is partitioned to shares and distributed to authorities by Shamir's secret key sharing scheme. This scheme satisfies fairness.
- Inalterability and privacy of voters are quaranteed by Paillier scheme.

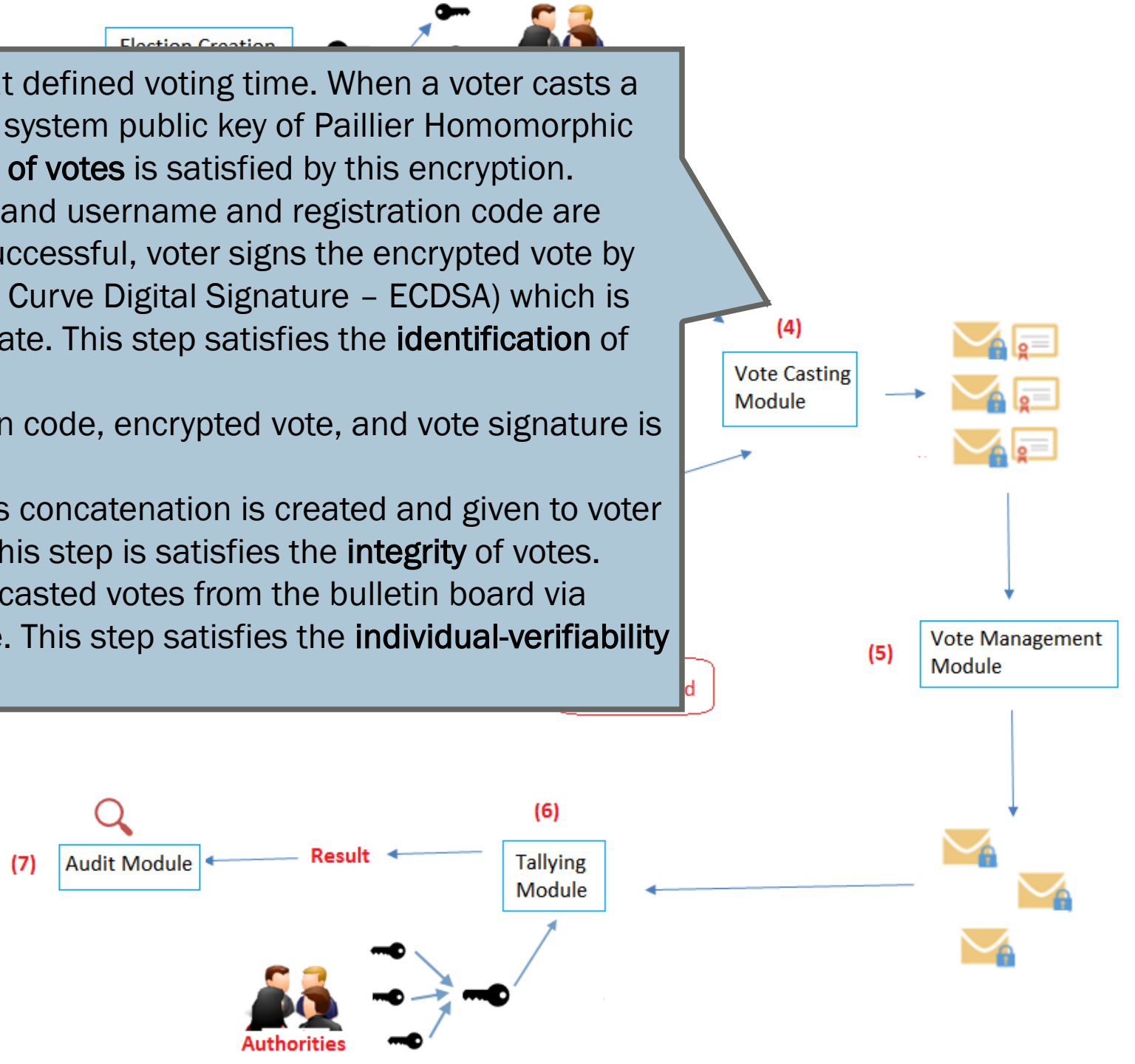


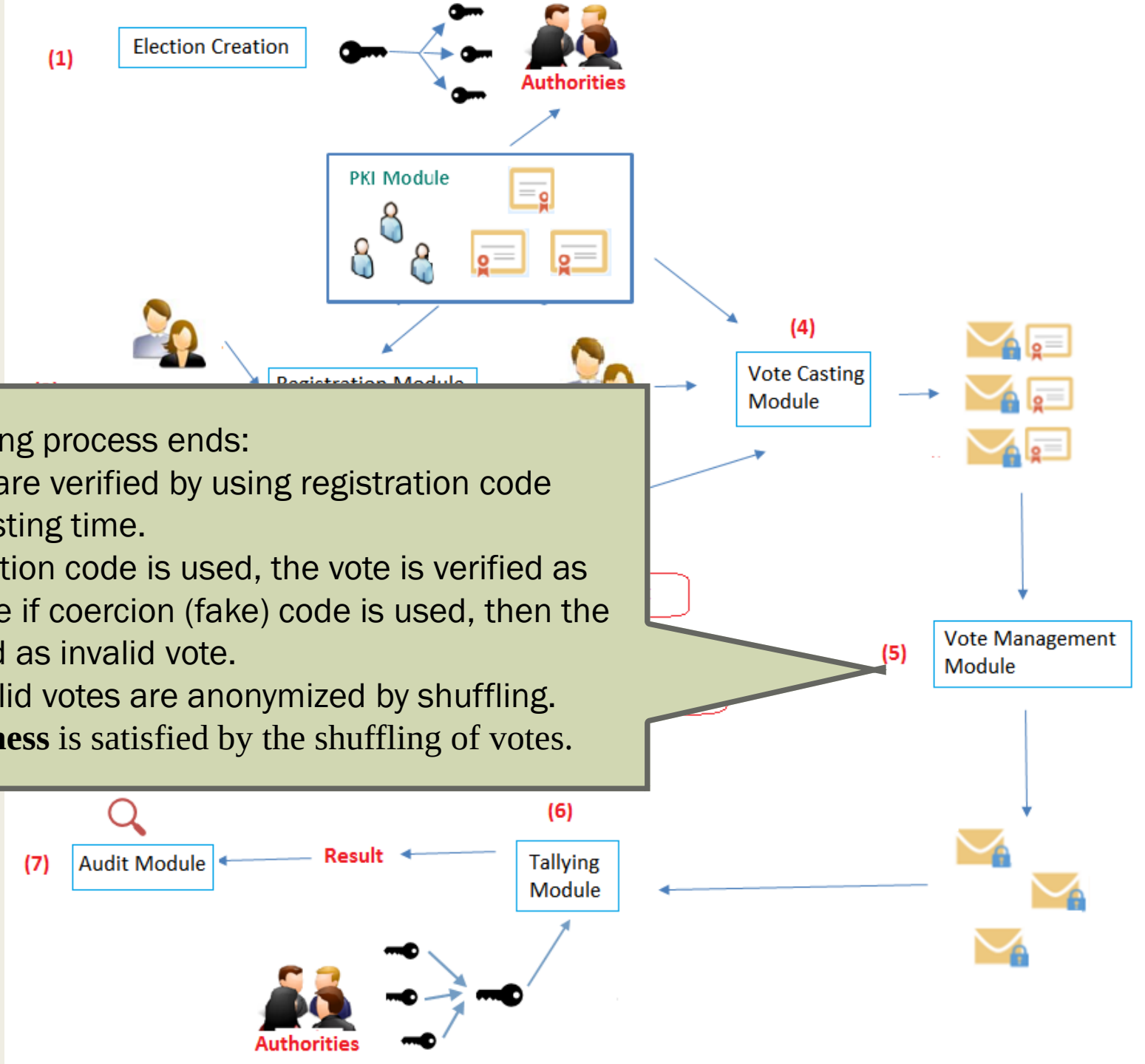
- This process starts at predefined registration time.
- Eligible voters who want to cast a vote must register to system.
- System creates and gives a registration code for eligible vote and a fake **registration code** to detect coercion case for each registered voter.
- **Eligibility** and **Non-Reusability** are quaranteed by the given registration code.
- **Coersion-resistancy** is satisfied by fake registration code.



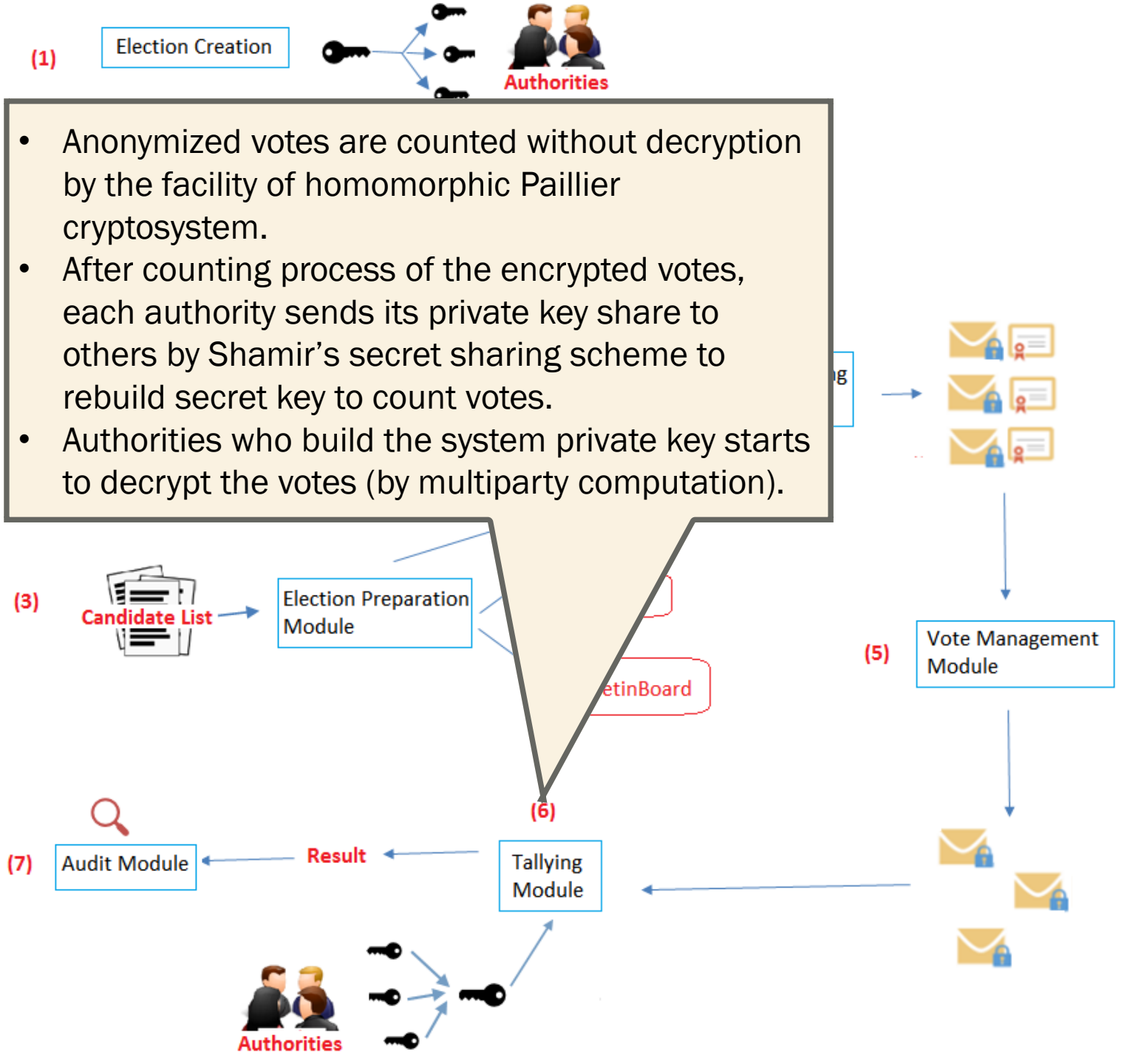
- Election preparation process starts.
- Predefined candidates are obtained from database as candidate list and
- An identification number is given for each candidate.
- The ballot that contains the list of candidates is created.
- The number of all eligible voters is counted.
- At last; a bulletin board is created and these information is announced.

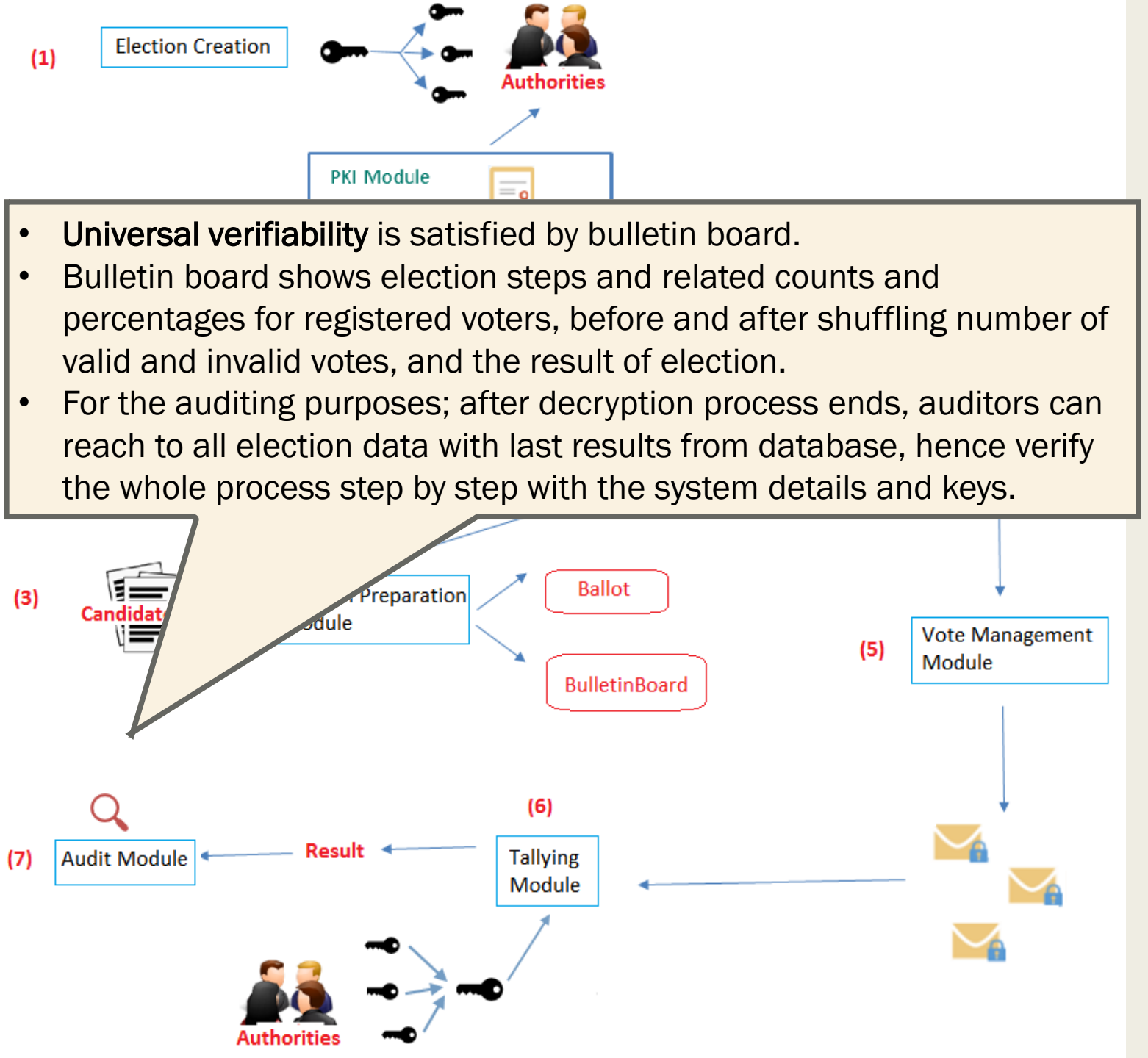
- Voting process starts at defined voting time. When a voter casts a vote, it is encrypted by system public key of Paillier Homomorphic Cryptosystem. **Secrecy of votes** is satisfied by this encryption.
- Login panel is opened and username and registration code are asked. If the login is successful, voter signs the encrypted vote by her private key (Elliptic Curve Digital Signature – ECDSA) which is related her PKI certificate. This step satisfies the **identification** of voter.
- Hash of the registration code, encrypted vote, and vote signature is concatenated.
- Then hash value of this concatenation is created and given to voter for tracking her vote. This step is satisfies the **integrity** of votes.
- Voters can query their casted votes from the bulletin board via using given hash value. This step satisfies the **individual-verifiability** of vote by voter.





- When the voting process ends:
- Casted votes are verified by using registration code entered at casting time.
- If real registration code is used, the vote is verified as valid vote, else if coercion (fake) code is used, then the vote is verified as invalid vote.
- Thereafter, valid votes are anonymized by shuffling.
- **Receipt-Freeness** is satisfied by the shuffling of votes.


(1)
Election Creation
Authorities
Anonymized votes are counted without decryption by the facility of homomorphic Paillier cryptosystem.
After counting process of the encrypted votes, each authority sends its private key share to others by Shamir's secret sharing scheme to rebuild secret key to count votes.
Authorities who build the system private key starts to decrypt the votes (by multiparty computation).
(3)
Candidate List
Election Preparation Module
etinBoard
(5)
Vote Management Module
(6)
(7)
Audit Module
Result
Tallying Module
Authorities



- **Universal verifiability** is satisfied by bulletin board.
- Bulletin board shows election steps and related counts and percentages for registered voters, before and after shuffling number of valid and invalid votes, and the result of election.
- For the auditing purposes; after decryption process ends, auditors can reach to all election data with last results from database, hence verify the whole process step by step with the system details and keys.

Conclusion

- https://github.com/Edu-Voting/e-voting-project
- Our system has been built with educational purposes by implementing cryptographic algorithms, taking into consideration requirements of e-voting system and basic security functions.
- Different homomorphic solutions can be also tested with this modular design and measure their efficiencies.

THANK YOU