Protection Profile for e-voting systems

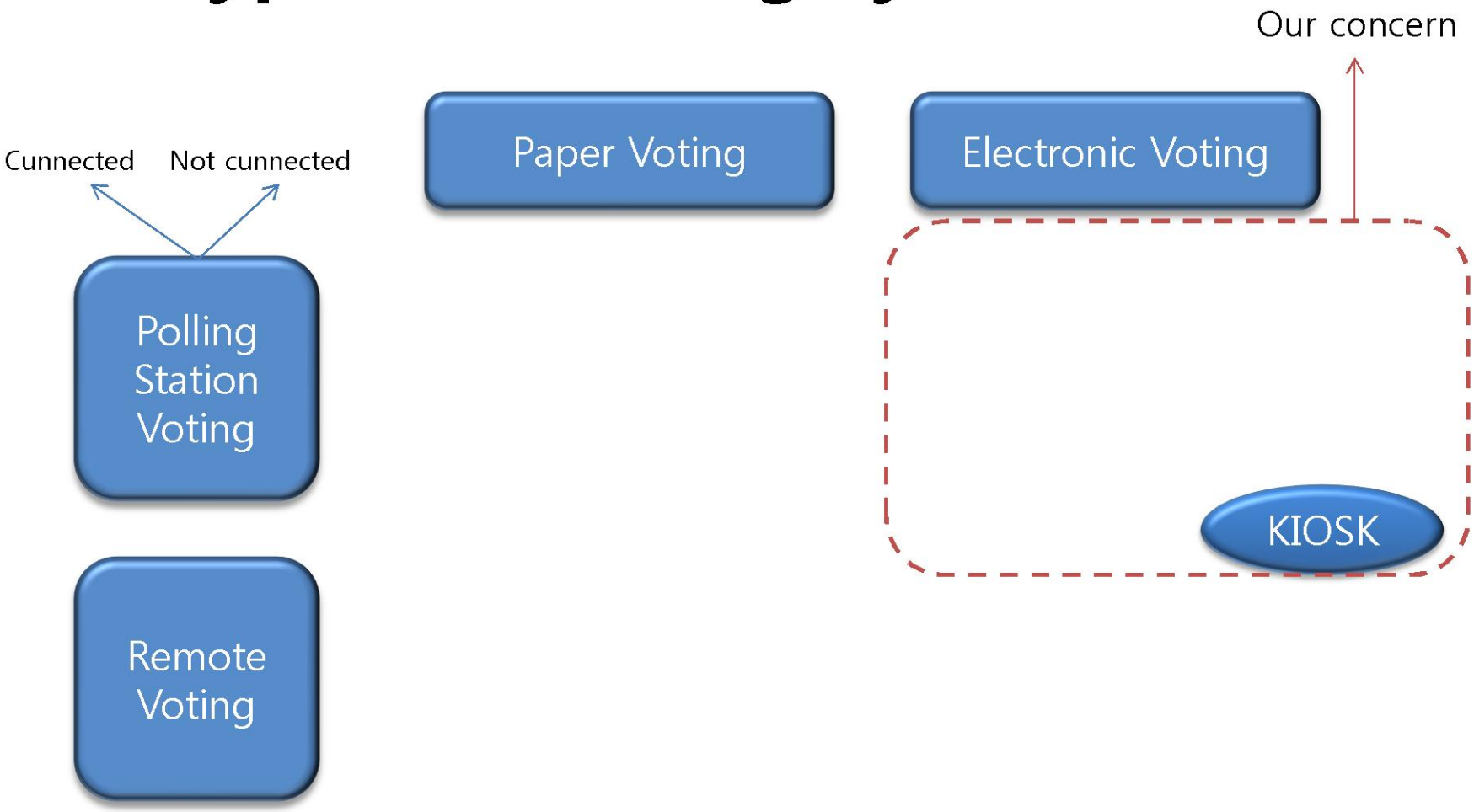
Kwangwoo Lee, Yunho Lee, Woongryul Jeon,
Dongho Won, Seungjoo Kim
Sungkyunkwan University, Information Security Group, Korea
http://security.re.kr



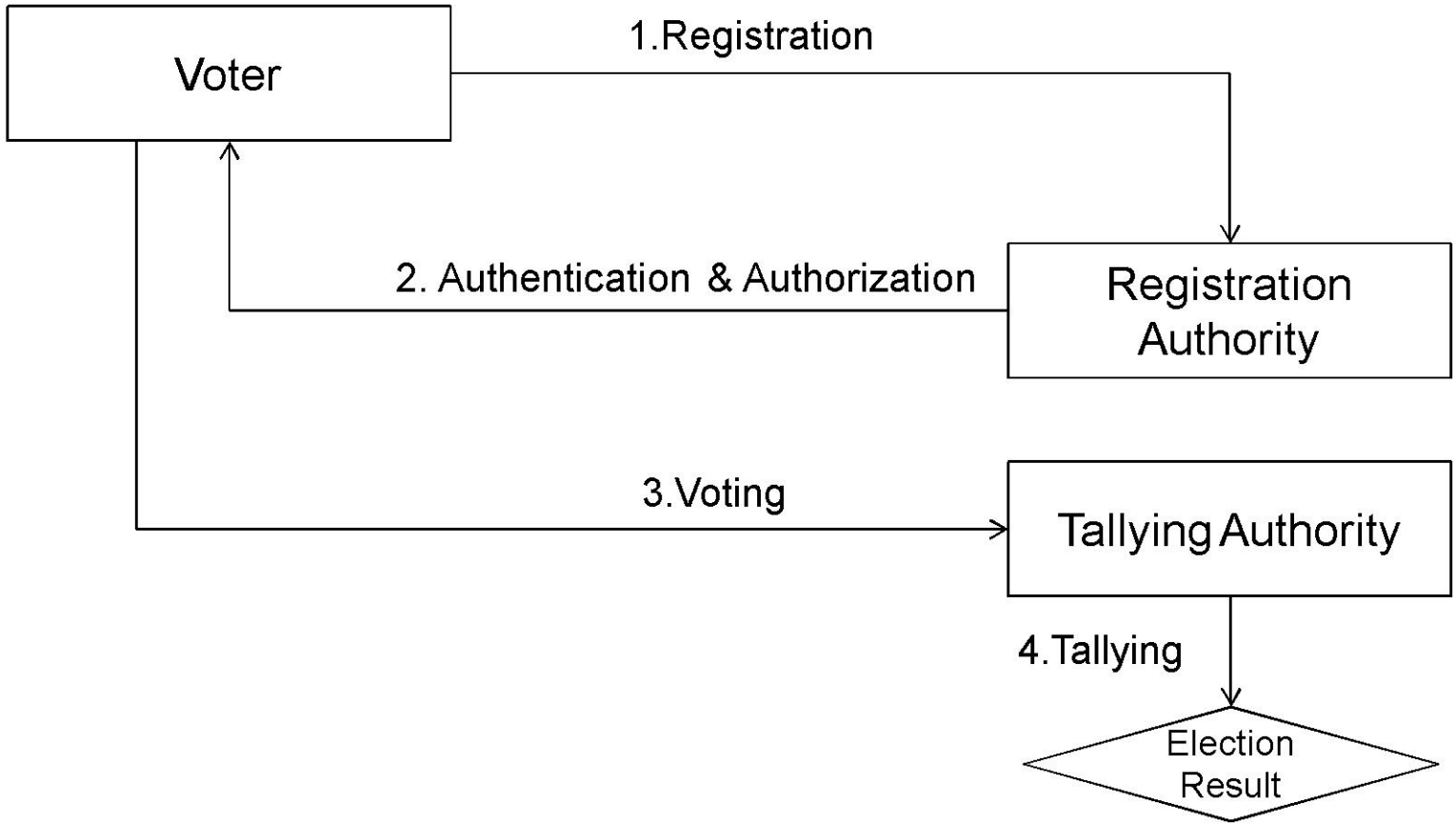
Why we use the e-voting system?

- Many counties try to adopt the e-voting machine in their election
  - Argentina, Australia, Austria, Belgium, Bosnia and Herzecobina, Brazil, Canada, Costa Rica, Finland, France, Germany, India, Japan, Korea, Netherlands, Portugal, Slovakia, Spain, Sweden, Swiss, United Kingdom, United States, Venezuela, etc.
- What is the advantages of e-voting system?
  - Accurate and fast tabulation of votes
  - Low cost
  - Improved accessibilty

The type of e-voting system



General Process of e-voting



Election Actors

- Voter
  - Voter has the right for voting, and he votes in the election
- Registration Authority
  - Registration authorities register eligible voters before the election day. These authorities ensure that only registered voters can vote and they vote only once on the election day. Registration authorities may be registrar authenticator, authorizer, ballot distributor and/or key generator
- Tallying Authority
  - The tallying authorities collect the cast votes and tally the results of the election. Tallying authorities may be counter, collector, or tallier

Election Phases

- Registration
  - Voters register themselves to registration authorities and the list of elibible voters is compliled before the election day
- Authentication and Authorization
  - On the election day registerd voters request ballot or voting privilege from the registration authorities. Registration authorities check the credentials of those attempting to vote and only allow those who are eligible and registerd befor
- Voting
  - Voter casts his vote
- Tallying
  - The tallying authorities count the votes and announce the election results

General Security Requirements

Security Requirements	Description
Completeness	All valid votes are counted correctly
Soundness	The dishonest voter cannot disrupt the voting
Privacy	All votes must be secret
Eligibility	No one who is not allowed to vote can vote
Unreusability	No voter can vote twice
Fairness	Noting must affect the voting
Verifiability	No one can falsify the result of the voting

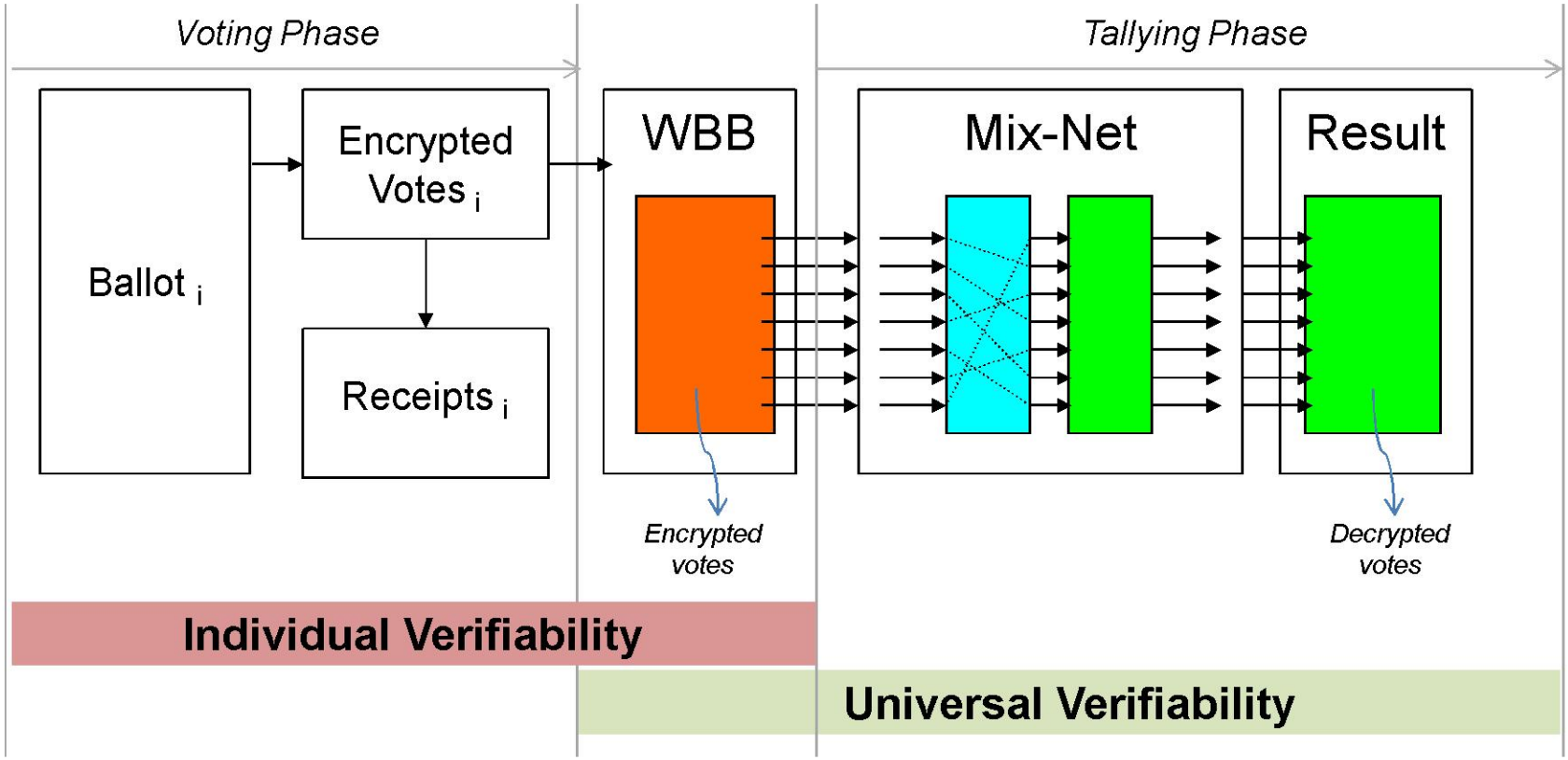
Problems

- Can you believe the result?
- How do you reflect your belief in its accuracy?
- Many of voters cannot believe the black-box e-voting machines
- To overcome these problems, many contries are trying to evaluate the e-voting system using the CC
- It can reduce risks and make voter to trust the election result

Verifiable e-voting

- Individual verifiability
  - A voter should be able to satisfy him/herself that the voted ballot has been captured correctly *(cast-as-intended)*
- Universal verifiability
  - Anyone should be able to satisfy him/herself that the voted ballot is counted correctly *(counted-as-cast)*

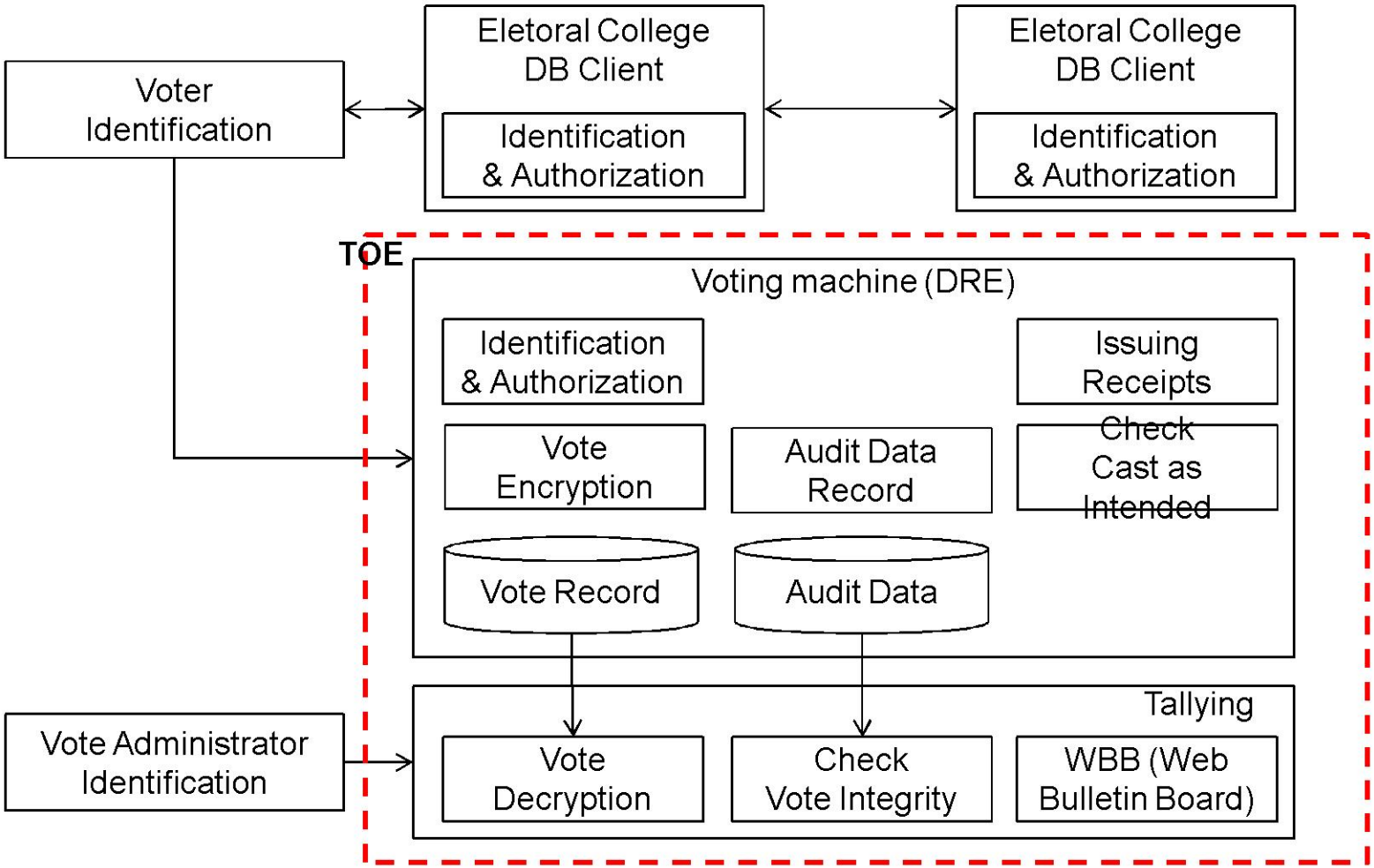
Implementation of Verifiable e-voting system



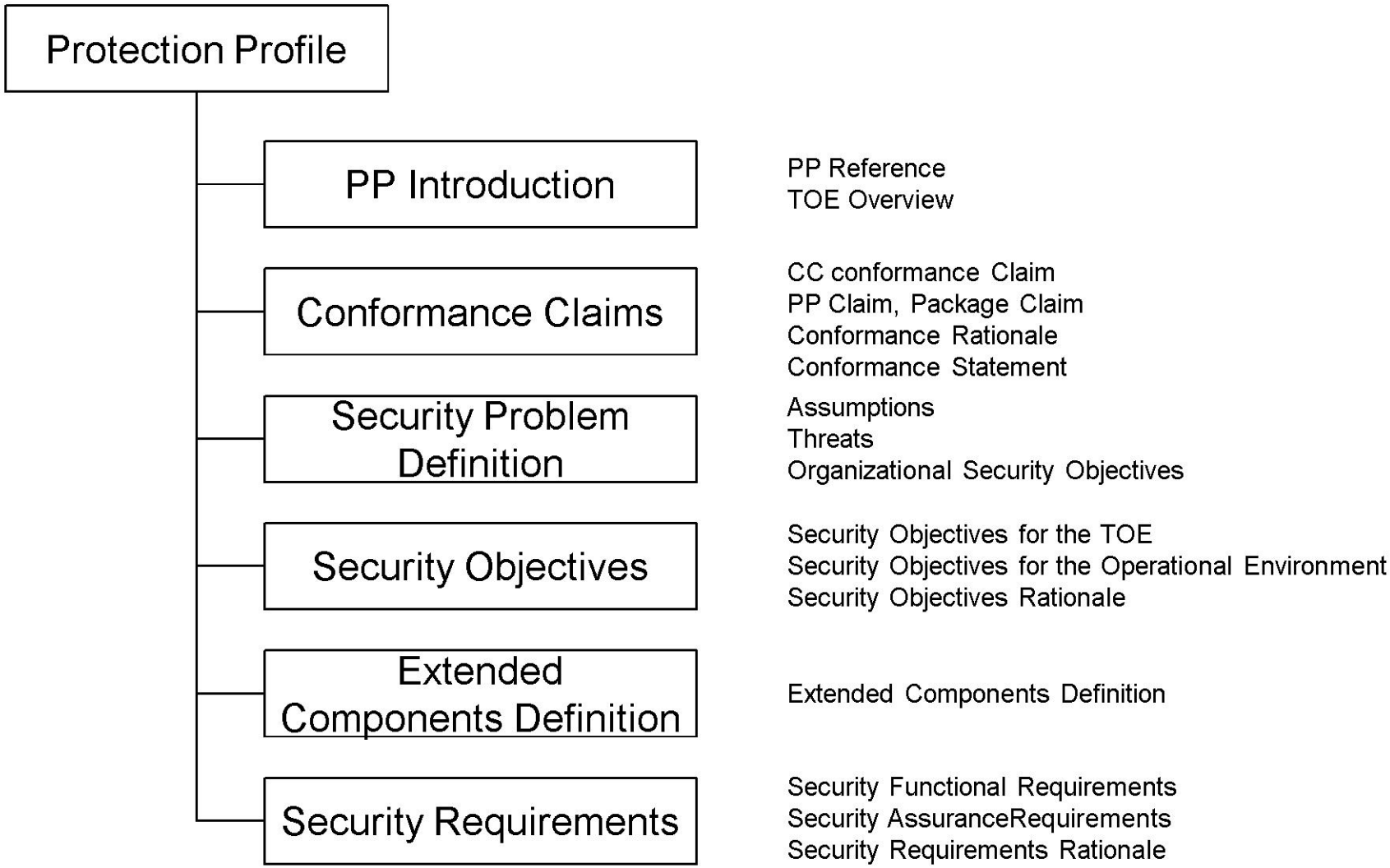
The Existing Protection Profiles

Protection Profile	BSI-PP-0031	PP-CIVIS	IEEE P1583
EAL	EAL3+	EAL2+	ELA2
CC version	CC v2.3	CC v3.0	CC v2.3
Voter verifiability	No	No	No
TOE boundary	Digital pen election system	DRE machine	DRE machine
Feature	This PP uses an electric digital pen to record a vote	Only this PP is listed in common criteria portal website	Voter cannot verify his/her vote

TOE (Target of Evaluation)



The Contents of Protection Profile



Threats (1/2)

Threats	Description
T.Malfunction	Users can cause malfunction like re-installation, and/or initialization of e-voting system.
T.Unexpected Events	E-voting can loss audit record by unexpected events like hardware, software and/or storage devices fault.
T.Unautherized System Modification	Unauthorized modification of the system, affecting operational capabilities, can be occurred.
T.Audit Record Alteration	Alteration of voting system audit record can be occurred.
T.Voting Record Alteration	Alteration of the recording of vote can be occurred.
T.Recording Prevention	Prevention of recording can be occurred.
T.Unautherized voting	Duplicate or fraudulent vote can be occurred.

Threats (2/2)

Threats	Description
T.System Data Alteration	Alteration of system data can be occurred.
T.Voting Data Exposure	Authorized or otherwise access can expose selection of voter.
T.New Vulnerability	Attacker can use new vulnerabilities not reported to gain access to e-voting system.
T.Recording Failure	Because of storage limitation, audit data may fail to be record.
T.TSF data tampering	Attacker can modify TSF data in unauthorized way to avoid record or cause misusage.
T.Bypass	Attacker can bypass the TOE security functions.
TE.Management	Administrator can threat the TOE security by insecure management, configuration, and operation.
TE.Delivery	The TOE can be harmed in delivery process.

Assumptions

Assumptions	Description
A.Physical	It is assumed that appropriate physical security is provided for the TOE and protects from unauthorized physical access by outsider.
A.Secure Installation and Operation	It is assumed that operating system of TOE is installed and managed in secure way.
A.Trusted Administrator	It is assumed that administrator are non-hostile, well trained and follow all administrator guidance.
A.Network	It is assumed that network service for TOE is based on secure communication protocols to ensure the identification and authentic of authorized system.
A.Connect	It is assumed that all connections to peripheral devices reside within the controlled access facilities.
A.Timestamp	It is assumed that TOE environment provides secure timestamp fulfill RFC 1305.

Organizational Security Policy(OSP)

Policies	Description
P.Audit	TOE must audit every auditable event and keep the audit record secure. This audit record is protected from unauthorized access.
P.Secure Managmenet	Authorized administrator must manage the TOE, audit log and so on forth in secure way.
P.Manager	Management rights must be given administrator authorized by election officials.
P.Alert	TOE activity must be monitored and an auditable or visual notification must be provided to an authorized administrator.
P.Alert Report	Documented procedures must be implemented for responding to and reporting violations of the TOE.
P.Authorized User	A voter must be authorized before voting.
P.Contingency Plan	A documented plan to maintain continuity of operation in an emergency or disaster must be given.
P.Data Authentication	Voting data must be authorized to verity its integrity.
P.Recover	The TOE must be capable of being restored to a secure state without losing any fatal data.
P.Test	The TOE and its associated documentation must demonstrate that it is an accurate implementation of a voting system.

Security Objectives for the TOE

Security Objectives	Description
O.Voter Authentication	An individual that has been determined to be a registered voter and is authorized to vote in the current election.
O.Encryption	The TOE must encrypt election data that is transmitted over a public network to protect against unauthorized access or modification.
O.Alert	The TOE must sound an alarm when a violation to a security policy has occurred.
O.Install	The TOE is delivered, installed, managed and operated in a manner that maintains security objectives.
O.Vote Validation	The TOE must ensure that votes recorded are verified by the voters as their intended vote prior to recording the vote.
O.Restore	The TOE must be capable of being restored to a secure state without losing the results of previously entered CVRs in the event of a disruption to normal operation.
O.Duplicate	The TOE must prevent duplicate.

Security Objectives for the TOE

Security Objectives	Description
O.Self Protection	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.Test	The TOE must support testing of its security functions.
O.Audit	The TOE must provide a means to record readable audit record of security related events, with accurate dates, time, and events. Furthermore, the TOE must provide variable manners to refer audit record.
O.Update	The TOE must keep secure against new vulnerabilities.
O.Manage	The TOE must provide manners that maintain the TOE secure to administrator.
O.Identification and Authentication	The TOE must every user before any action.
O.TSF Data Protection	The TOE must protect TSF data from unauthorized exposure, alteration, and deletion.
O.Vote Verification	The TOE must provide manner for every voter to verity their intended vote.

Security Objectives for the Operational Environment

Security Objectives	Description
OE.Contingency Plan	A contingency plan and associated procedure for emergency situations must be in effect.
OE.Event Reporting	Procedures for responding to and reporting security violations of the TOE security policy must be implemented.
OE.Integrity	The TOE must prevent unauthorized modification of election data during creation, storage and transmission.
OE.Policy Documentation	Security policies for the TOE must be documented and distributed to all personnel responsible for implementation.
OE.Physical	Appropriate physical security must be provided for the TOE.
OE.Trusted Administrator	Authorized administrator must be trained as to establishment and maintenance of security policies in practice.
OE.Management	The TOE must be managed in way that maintains security policies.
OE.Access Point	Every transmission between user and database must pass through the TOE.
OE.Timestamp	The TOE environment must provide secure timestamp fulfill RFC 1305.

Security Functional Requirements

Class	Components
Security Audit (FAU_*)	GEN.1(Audit data generation), GEN.2(User identification association), SAA.1(Potential violation analysis), SAR.1(Audit review), SAR.2(Restricted audit review), SAR.3(Selectable audit review), STG.1(Protected audit trail storage)
Cryptographyic Support (FCS_*)	CKM.1(Cryptographic key generation), CKM.2(Cryptographic key distribution), CKM.3(Cryptographic key access), CKM.4(Cryptographic key destruction), COP.1(Cryptographic operation)
User Data Protection (FDP_*)	ACC.1(Subset access control), ACF.1(Security attribute based access control), DAU.1(Basic data authentication), DAU.2(Data authentication with identity of guarantor), ITT.1(Basic internal transfer protection), RIP.1(Subset residual information protection), RIP.2(Full residual information protection), SDI.1(Stored data integrity monitoring), UIT.1(Data exchange integrity)
Identification & Authentication (FIA_*)	ATD.1(User attribute definition), SOS.1(Verification of secrets), UAU.1(Timing of authentication), UID.2(User identification before any action)

Security Functional Requirements

Class	Components
Security Management (FMT_*)	MOF.1(Management of security functions behavior), MSA.1(Management of security attributes), MSA.2(Secure security attributes), MSA.3(Static attribute initialization), SMR.1(Security roles), SMR.2(Restrictions on security roles)
Privacy (FPR_*)	ANO.2(Anonymity without soliciting information), PSE.1(Pseudonymity)
Protection of the TSF (FPT_*)	AMT.1(Abstract machine testing), FLS.1(Failure with preservation of secure state), PHP.1(Passive detection of physical attack), RCV.1(Manual recovery), STM.1(Reliable time stamp), TST.1(TST testing)
Fault Tolerance (FRU_*)	RSA.2(Minimum and maximum quotas)
Trusted Path/Channel (FTP_*)	ITC.1(Inter-TSF trusted channel)

Security Assurance Requirements

- Our protection profile adopts EAL4+ level
- E-voting system is a critical information system
  - The result of attack can cause terrible confusion in society
- We extend security assurance requirements to reinforce verification of implementation
  - Extended requirements are ADV_IMP_2, ATE_DPT.3, AVA_VAN.4.

Comparison

PP	BSI-PP-0031	PP-CIVIS	IEEE P1583	The Proposed
EAL	EAL3+	EAL2+	EAL2	EAL4+
CC Ver.	CC v2.3	CC v.3.0	CC v.2.3	CC v.3.1
TOE	Digital pen, Docking station, Firmware, Software	DRE machine (hardware /software)	DRE machine (hardware /software)	DRE machine (hardware /software)
# of T.	7	1	13	15
# of A.	17	5	8	7
# of OSP.	4	22	21	10
VVAT	No	No	No	Yes

T : Threat A: Assumption OSP: Organizational Security Policy
VVAT: Voter Verifiable Audit Trail

Conclusion

- Many of voters cannot believe the black-box e-voting machines
- The PP for e-voting systems should consider the voter verifiability
- We proposed a protection profile of an e-voting system for evaluation against CC v3.1

Q & A