CS419 Virtual Election Booth

Billy Lynch wlynch92

Will Langford wtl17

Spring 2014

1 Protocol

Key:

V = Voter L = CLA = Central Legitimization Agency T = CTF = Central Tabulation Facility P = Publish

$\langle Name ValidationNumber (Name ValidationNumber)_{Sig_L})_{E_{KUV}}$	
$(Validation Number (Validation Number)_{Sig_L})_{E_{KUT}}$	
$(Validation Number Voter ID Vote)_{E_{KUT}}$	
$ACK (ACK)_{Sig_T}$	
1	
$(ID:Vote)_1 (ID:Vote)_2 (ID:Vote)_n$	
$(n VN_1 VN_2 VN_n (n VN_1 VN_2 VN_n)_{Sig_T})_{E_{KUL}}$	
$(n Name_1 Name_2 Name_n (n Name_1 Name_2 Name_n)E_{KUT}$	
$Name_1 Name_2 Name_n$	

2 System Design

3 Security Requirements

- Only authorized voters can vote. asdf
- No one can vote more than once.
- No one can determine for whom anyone else voted.
- No one can duplicate anyone else's votes.
- Every voter can make sure that his vote has been taken into account in the final tabulation.
- Everyone knows who voted and who didn't.