CS419 Virtual Election Booth

Billy Lynch wlynch92 Will Langford wtl17

Spring 2014

1 Protocol

Key:

V = Voter

L = CLA

T=CTF

P = Publish

$Name (Name)_{Sig_{V}}$	\longrightarrow
$(Name ValidationNumber (Name ValidationNumber)_{Sig_L})_{E_{KUV}}$	7
$(ValidationNumber (ValidationNumber)_{Sig_L})_{E_{KUT}}$	<u>></u>
$(Validation Number Voter ID Vote)_{E_{KUT}}$	
$\langle ACK (ACK)_{Sig_T}$	
$(ID:Vote)_1 (ID:Vote)_2 (ID:Vote)_n$	
$(n VN_1 VN_2 VN_n (n VN_1 VN_2 VN_n)_{Sig_T})_{E_{KUL}}$	\longrightarrow
$ \leftarrow (n Name_1 Name_2 Name_n (n Name_1 Name_2 Name_n)_{E_{KUT}} $	
$Name_1 Name_2 Name_n$	

- 2 System Desgin
- 3 Security Requirements