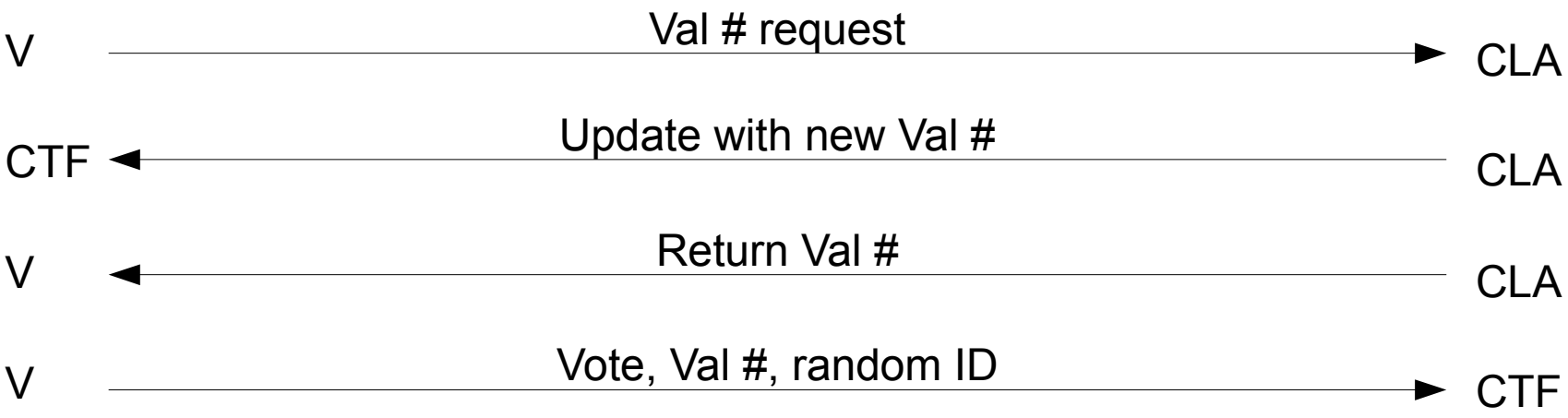
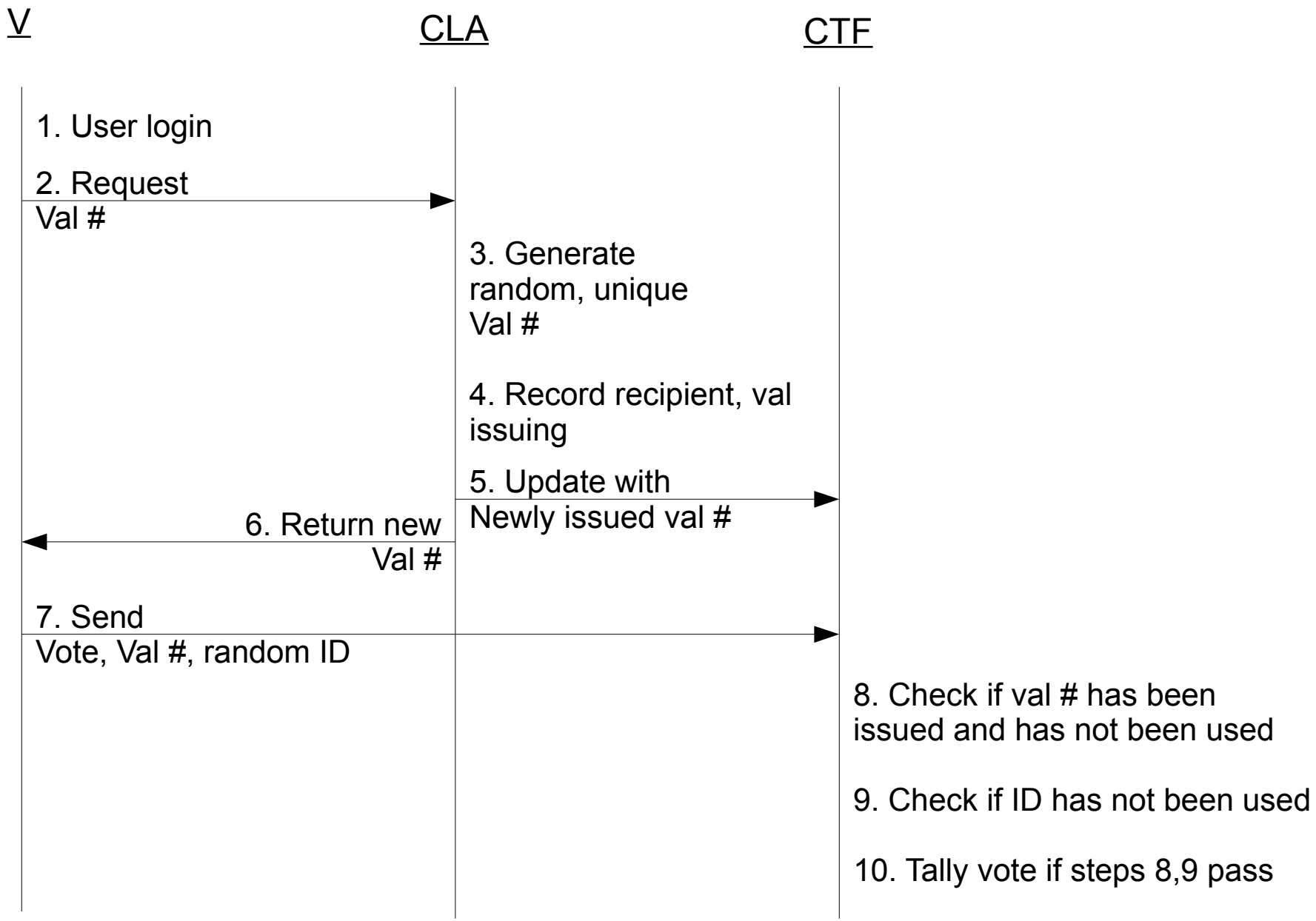
SECTION 1:


V
Val # request
CLA
CTF
Update with new Val #
CLA
V
Return Val #
CLA
V
Vote, Val #, random ID
CTF

Sample voting use case:



SECTION 2:

All communication between interfaces and servers is performed using SSL. We take the assumption that the CLA and CTF servers have successfully launched prior to voter communication.

Implementation of voter's interface:

The Voter will take the first step of logging in to the system using their name. This creates a simple text interface allowing them to either request a validation number or submit a vote. Entering "REQUEST VAL" will send information (including the recipient's entered login name) to the CLA server to begin the process of generating a new validation number. The CLA server will then reply back to the voter interface with the validation number and a list of candidates and their IDs for voting. (This validation number has been fixed to 4 digit entries for ease of use during the demo).

Next, the voter may enter "VOTE <voteid> VAL <valnum> ID <randomid>". This will send a message to the CTF to tally in the vote (may or may not pass, depending on validity of the validation number and availability of the random ID).

Implementation of CLA server:

Upon successful launch, the CLA server will wait for validation number requests from the voters. The random validation number is generated by the CLA (fixed to be no larger than 4 digits for ease of use). This validation number is checked for its uniqueness so that two of the same validation numbers are distributed. The CLA then records the validation number to have been used in an array, and the recipient's username in a hashtable. The newly generated validation number is then delivered to the CTF. The CLA finally responds to the voters request with a validation number assuming all checks have passed (checks including that the recipient has not received a validation number).

Implementation of CTF server:

The CTF waits for updates from the CLA for newly activated Validation numbers which are stored in an array. When a voter sends a vote for processing to the CTF, it check whether the validation number has been registered to be used and has not yet been used, and if the ID has not yet been used. It does with by checking a hashtable indexed by the voter's random ID, holding their vote and validation # used. If all checks pass, then the vote is counted with that random ID. In our system, once a cap of 5 votes has been reached, the CTF displays the results of ID+vote and all voters who participated in the voting with their username.

SECTION 3:

> Only authorized users can vote:

Users may only vote with a valid validation number. This number is random and large enough to resist brute force attacks. Without knowing that a particular validation number, it would be improbable for a malicious user to submit a vote with attempts of guessing validation numbers.

> No one can vote more than once: The CLA keeps track of users who requested validation numbers and does not distribute validation numbers to recipients of previous validation numbers. Validation numbers may only be submitted once each to the CTF. The CTF will deny any attempts to vote with validation numbers that have already been used to vote with.

> No one can determine for whom anyone else voted: Information for who voted is only stored with a random ID. There is no correlation between a username, their random ID, and the vote they submitted. Unless a random ID is compromised, it is not possible for them votes to be assigned to users.

> No one can duplicate anyone else's votes: Once a vote is received by the CTF, the validation number is crossed off and the random ID is marked as used. In the event of a replay attack on the CTF, it will reject the vote as it considers that the validation number has already been consumed, and that the submitted random ID is already used.

> Every voter can make sure that his vote is taken into account: Final tabulation is displayed when the cap is reached where voters may recognize their vote with the random ID they submitted. No duplicate ID's are permitted, so a user is guaranteed the ability to distinguish his or her vote from the rest.

> Everyone knows who voted and who didn't: All voters' who participated in the voting will have their username displayed and recognized upon reaching the end of the voting session.

Written by: Komail Dharsee, Nawal Velez