ASIAN '07

“Browser-based Agile E-Voting ”

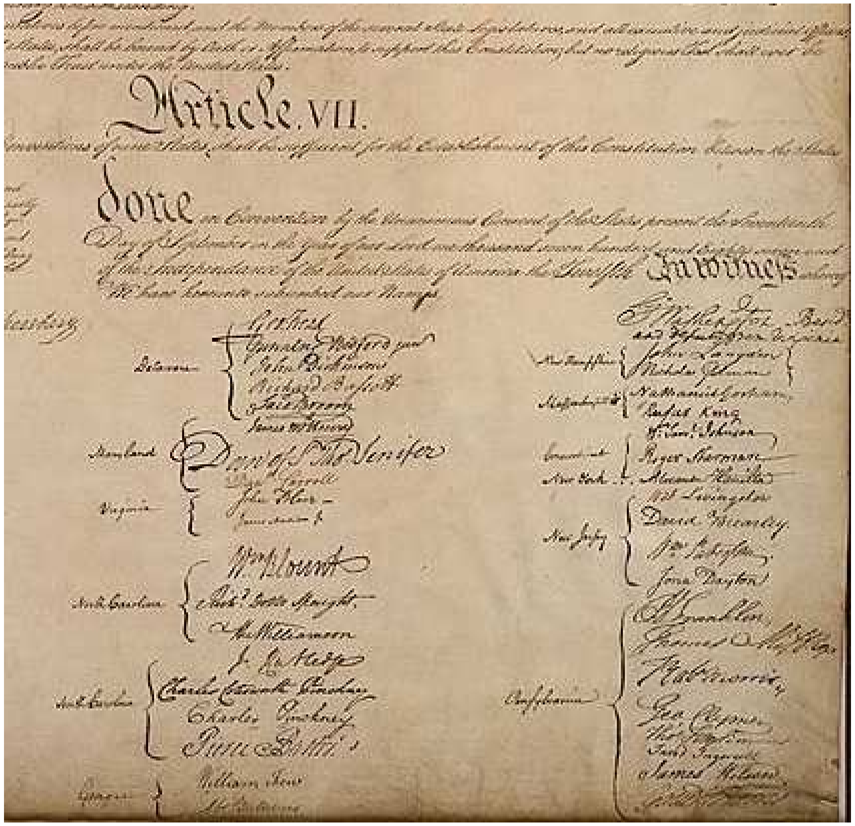
prepared by

Sriperumbuduru Kandala Simhalu
(Carnegie Mellon CyLab, Japan)

Keiji Takeda
(Carnegie Mellon CyLab, Japan)

December 2007

Power of, by and for the people



Article. VII.

done

In Witness

EVoting Security Requirements

- ➔Privacy

- ➔Verifiability
- ➔Individual Verifiability
- ➔Universal Verifiability

- ➔Receipt-freeness

- ➔In-coercibility

- ➔Fairness

Courtesy: Krishna Sampigethaya and Radha Poovendran: "A Framework and Taxonomy for Comparison of Electronic Voting Schemes".

Agile E-voting
(Quick bite)

→Voter Participation
Login-free

→Individual Verifiability
Additional Random Number selection

Related Research Work

➔Neff, C.A.: Practical high certainty intent verification for encrypted votes. (2004)

➔Reynolds, D.J.: A method for electronic voting with Coercion-free receipt.(2005)

➔Moran, T., Naor, M.: Receipt-Free Universally-Verifiable Voting With Everlasting Privacy. (2006)

Related Practical Applications

- ADDER

  It is an homomorphic-based remote Internet voting system.

  [Aggelos Kiayias,Korman Michael ,Walluck David :"An Internet Voting System Supporting User Privacy" (2006)]

- CIVS

  Condorcet Internet Voting Service.

  It is a ranking based free e-voting system.

  http://www.cs.cornell.edu/andru/civs.html.

- KOA

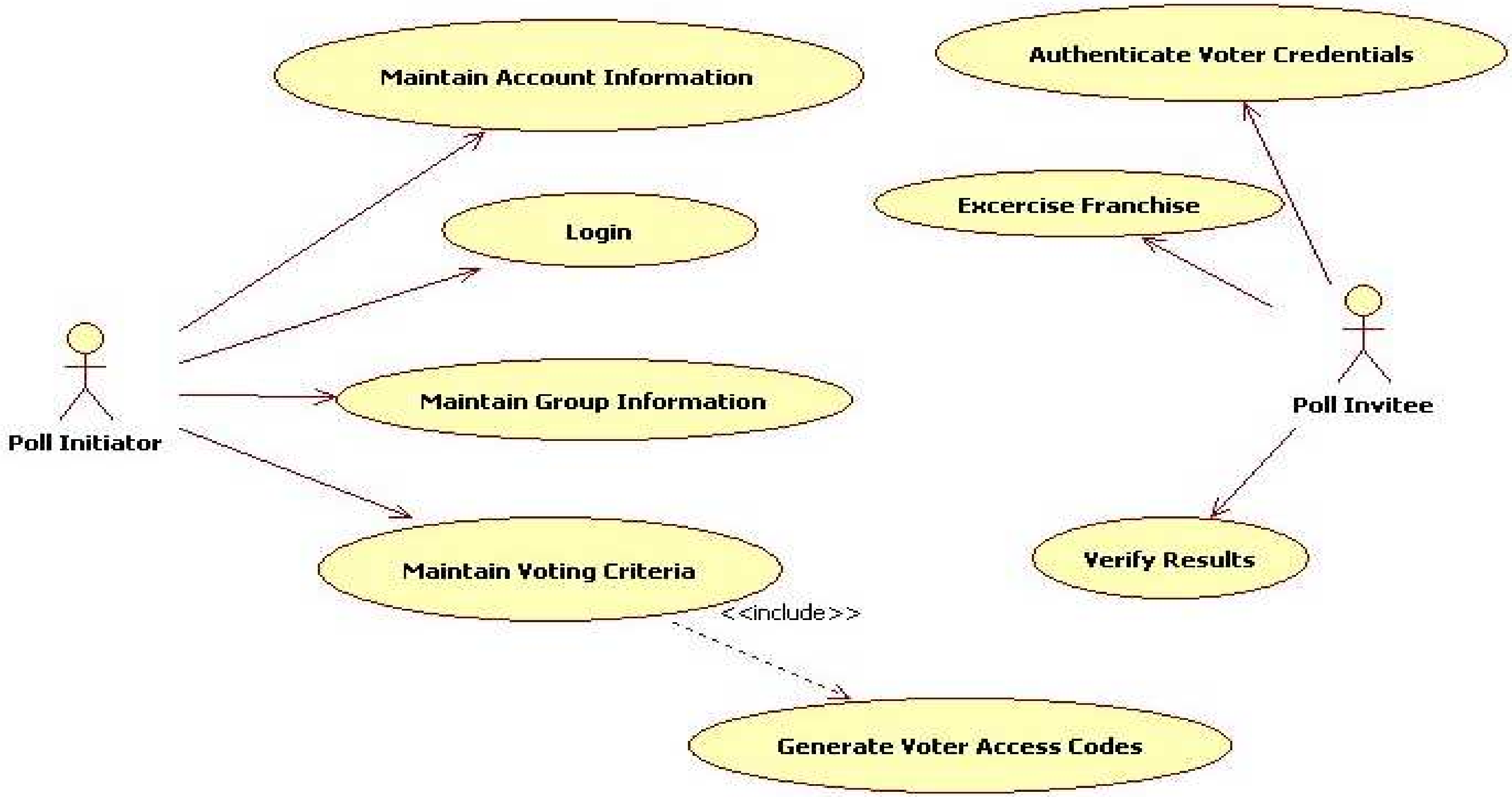
  The KOA system is the first Free Software Internet voting system developed, which was used for a government election.

  [J. Kiniry, A. Morkan, D. Cochran, F. Fairmichael, P. Chalin, M. Oostdijk, and E. Hubbers.: "The KOA remote voting system: A summary of work to date." (2006)]

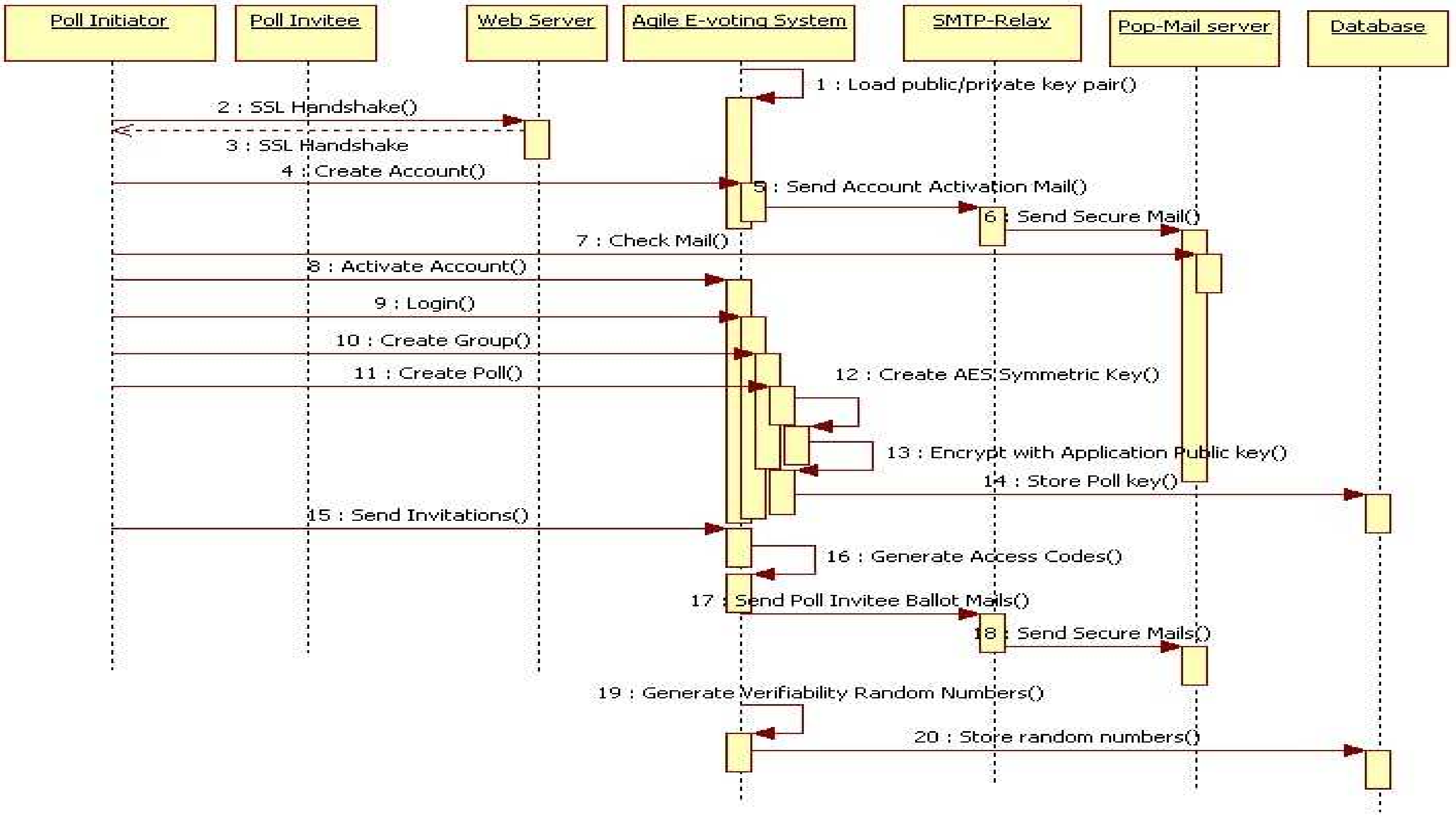
Project Overview-*The Agile Way*

- ➔Login-free voting
- ➔Integrated with regular e-mail usage
- ➔Targeting groups, e.g. Project groups, Friends' circle..
- ➔Scrum Master' Approach – the Agile Way
- ➔User Friendliness/Convenience

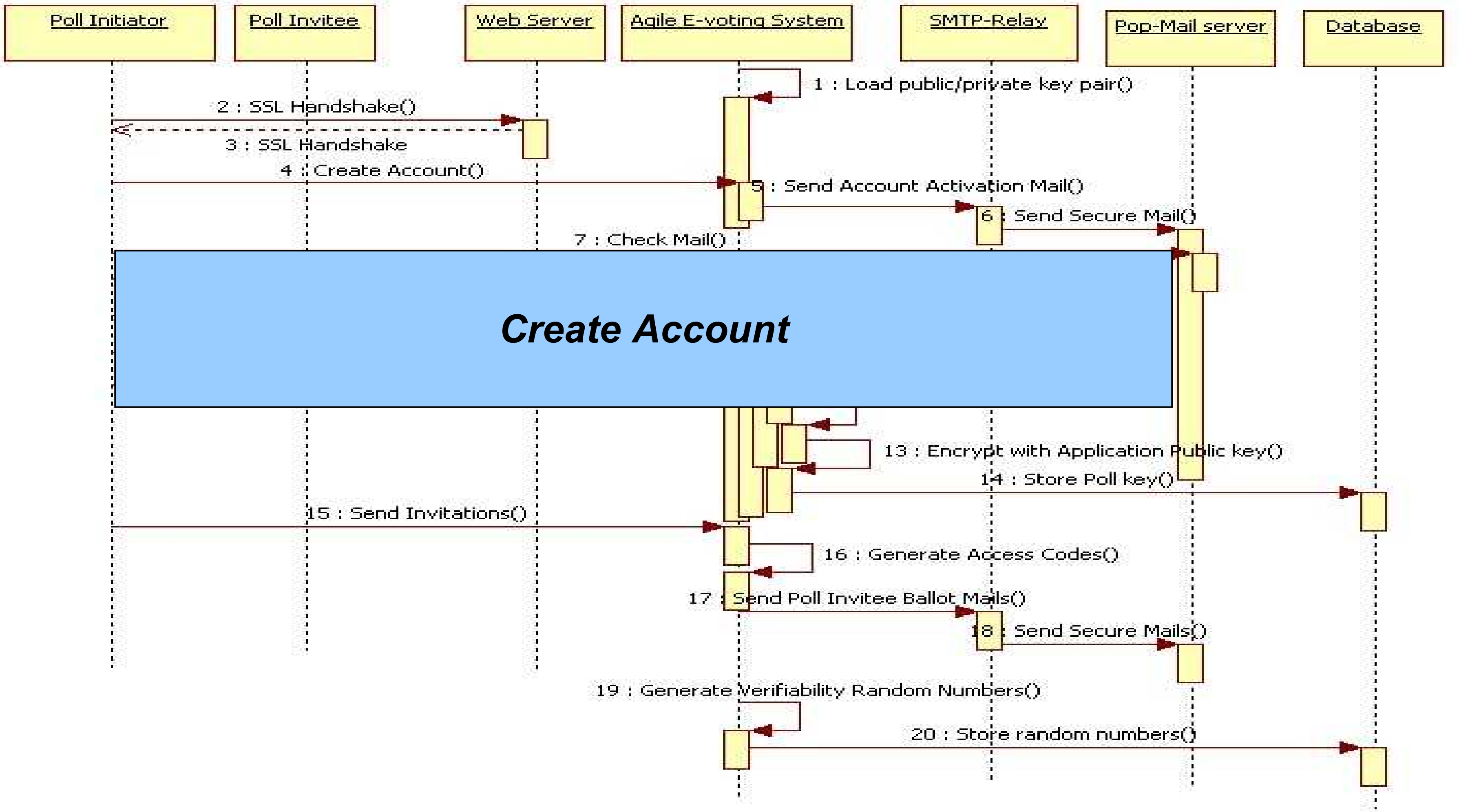
Overview – Use Case


Maintain Account Information
Authenticate Voter Credentials
Login
Excercise Franchise
Poll Initiator
Maintain Group Information
Poll Invitee
Maintain Voting Criteria
Verify Results
<<include>>
Generate Voter Access Codes

Poll Initiator Interactions[1/9]

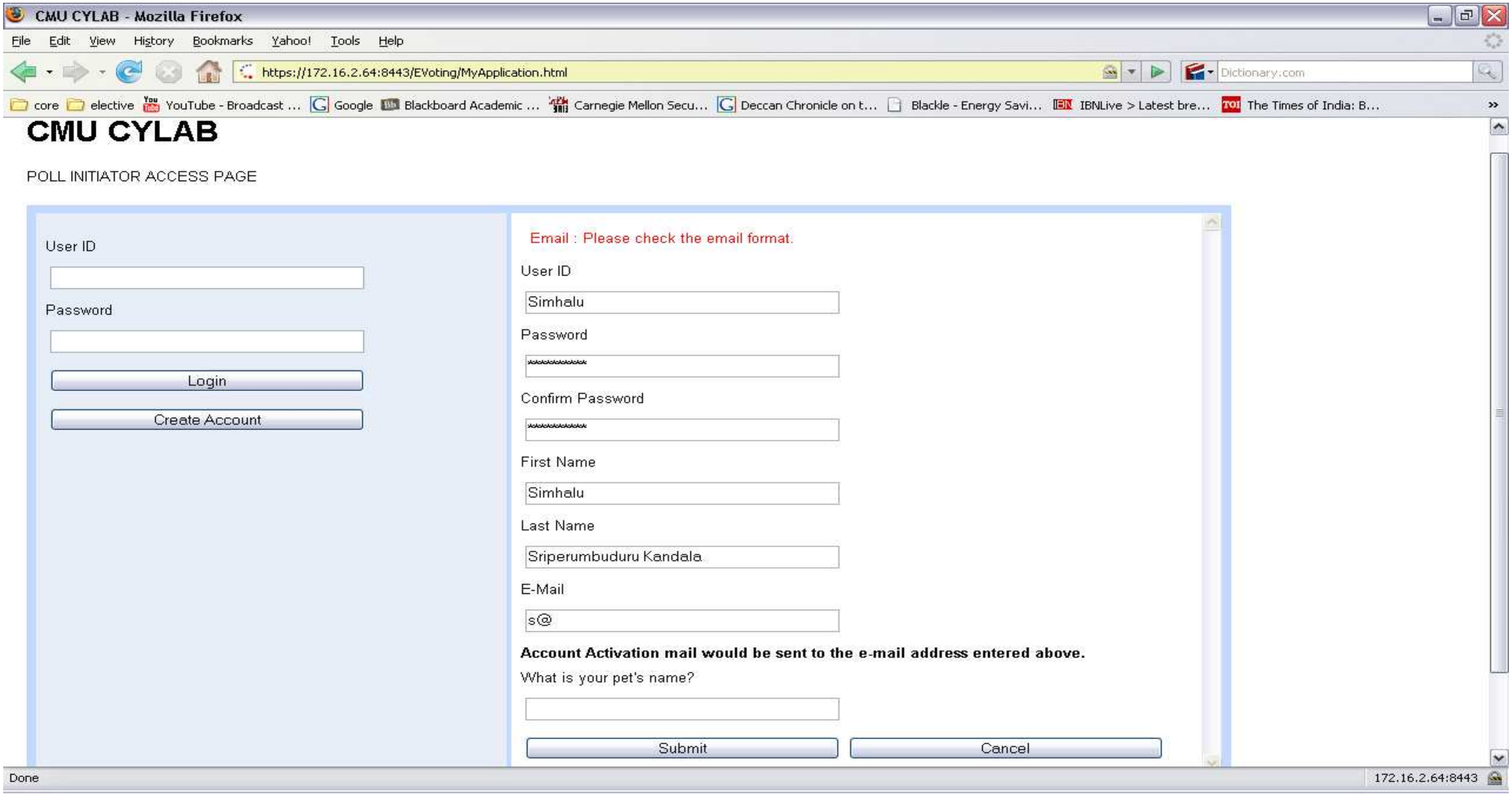


Poll Initiator Interactions[2/9]



Create Account

Poll Initiator Interactions[3/9]



CMU CYLAB - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://172.16.2.64:8443/EVoting/MyApplication.html
Dictionary.com
core elective YouTube - Broadcast ... Google Blackboard Academic ... Carnegie Mellon Secu... Deccan Chronicle on t... Blackle - Energy Savi... IBNLive > Latest bre... The Times of India: B...
Done
172.16.2.64:8443

CMU CYLAB

POLL INITIATOR ACCESS PAGE

User ID

Password

Login

Create Account

Email : Please check the email format.

User ID: Simhalu

Password: ***********

Confirm Password: ***********

First Name: Simhalu

Last Name: Sriperumbuduru Kandala

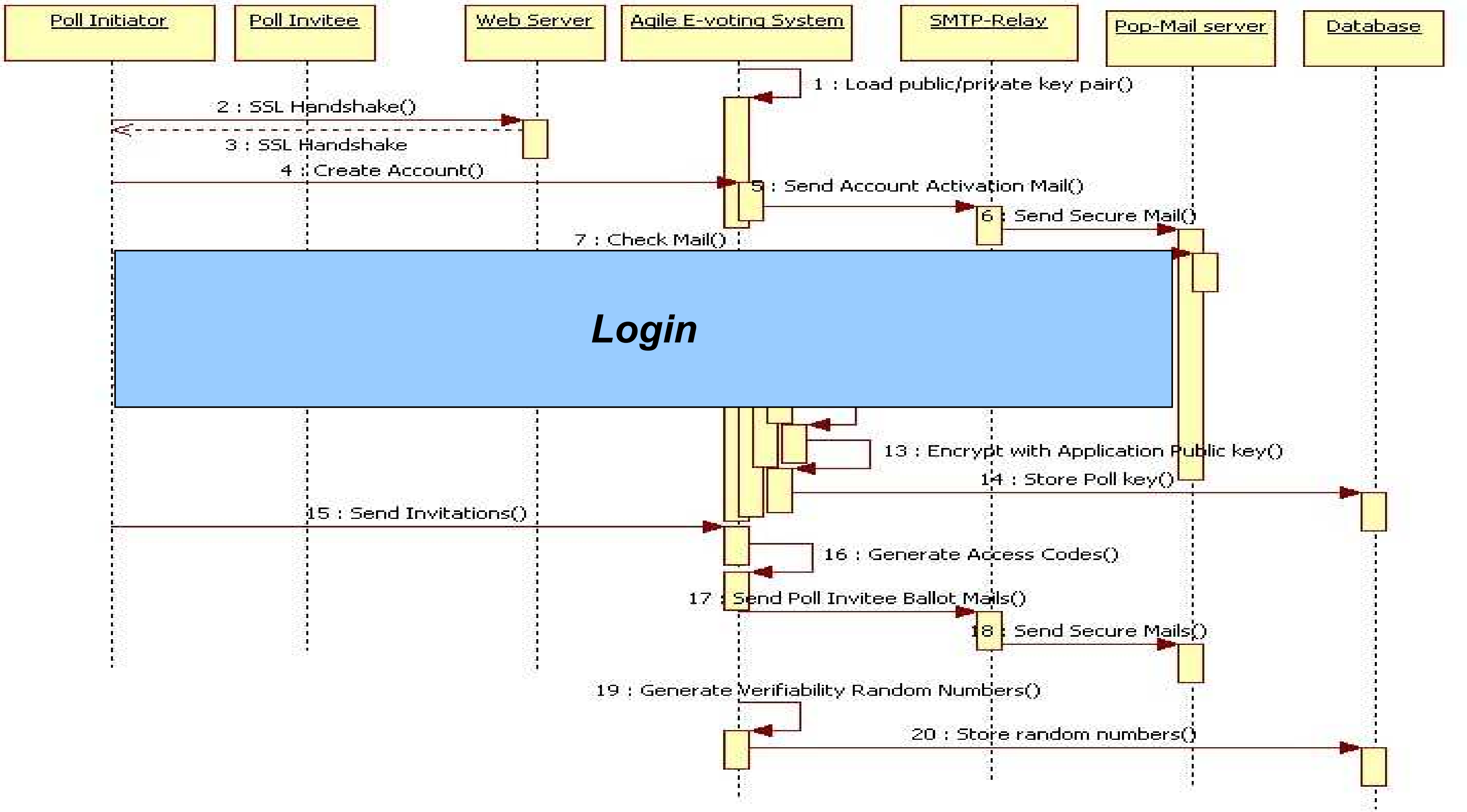
E-Mail: s@

Account Activation mail would be sent to the e-mail address entered above.

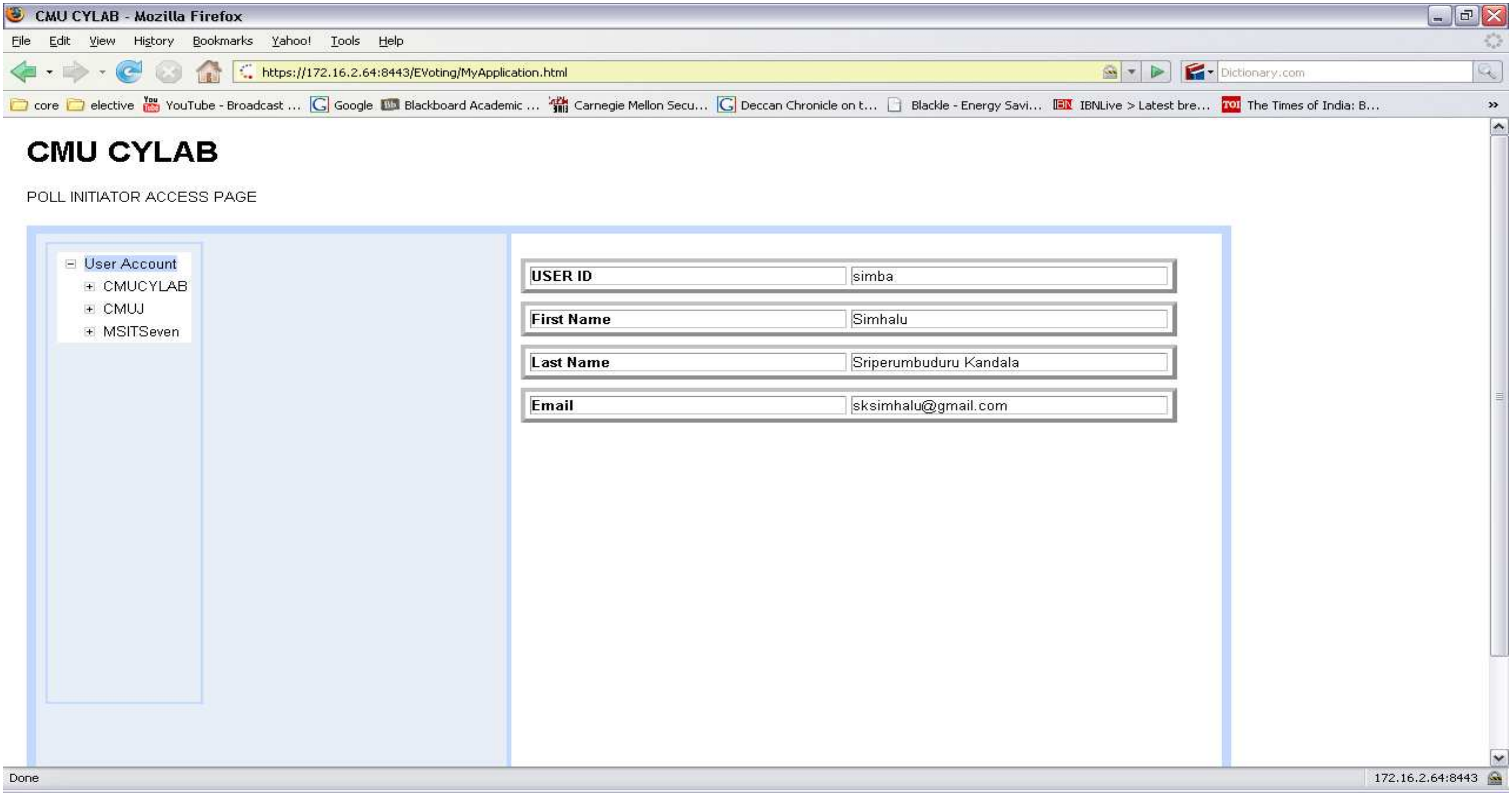
What is your pet's name?

Submit Cancel

Poll Initiator Interactions[4/9]



Poll Initiator Interactions[5/9]



CMU CYLAB - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://172.16.2.64:8443/EVoting/MyApplication.html
Dictionary.com
core elective YouTube - Broadcast ... Google Blackboard Academic ... Carnegie Mellon Secu... Deccan Chronicle on t... Blackle - Energy Savi... IBNLive > Latest bre... The Times of India: B...
Done
172.16.2.64:8443

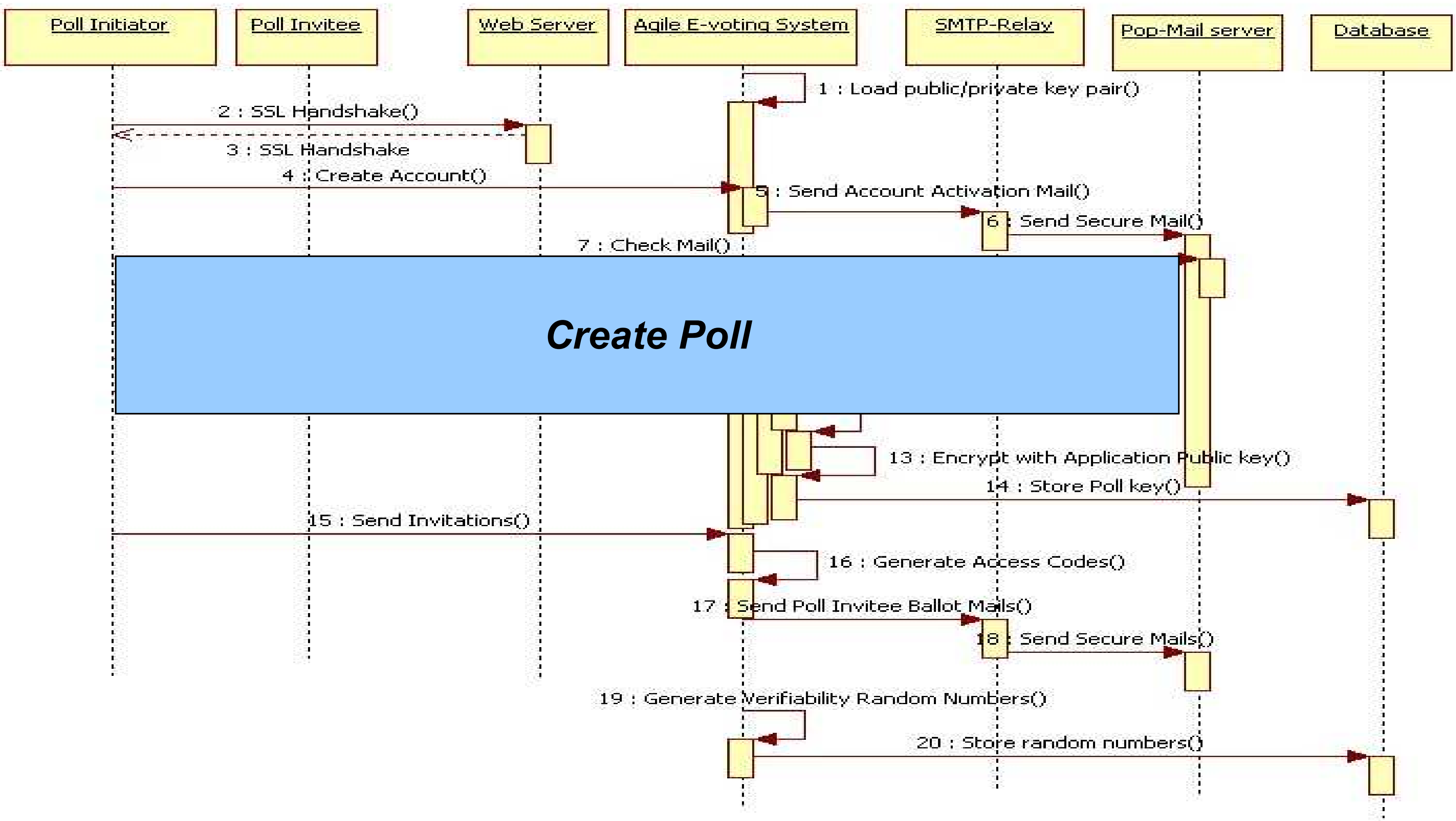
CMU CYLAB

POLL INITIATOR ACCESS PAGE

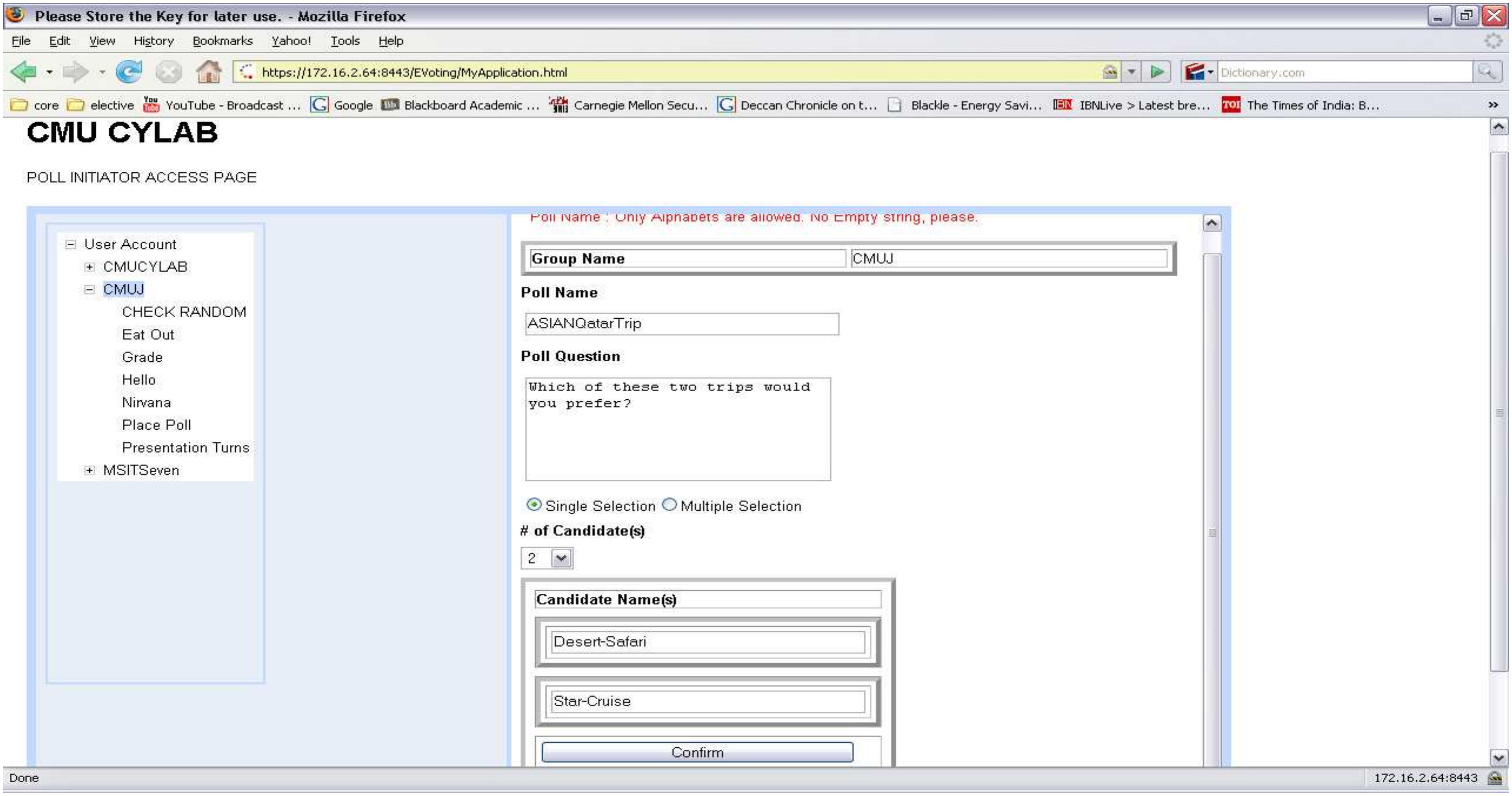
- User Account
  - CMUCYLAB
  - CMUJ
  - MSITSeven

USER ID	simba
First Name	Simhalu
Last Name	Sriperumbuduru Kandala
Email	sksimhalu@gmail.com

Poll Initiator Interactions[6/9]



Poll Initiator Interactions[7/9]



Please Store the Key for later use. - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://172.16.2.64:8443/EVoting/MyApplication.html
Dictionary.com
core elective YouTube - Broadcast ... Google Blackboard Academic ... Carnegie Mellon Secu... Deccan Chronicle on t... Blackle - Energy Savi... IBNLive > Latest bre... The Times of India: B...
Done
172.16.2.64:8443

CMU CYLAB

POLL INITIATOR ACCESS PAGE

- User Account
  - CMUCYLAB
  - CMUJ
    - CHECK RANDOM
    - Eat Out
    - Grade
    - Hello
    - Nirvana
    - Place Poll
    - Presentation Turns
  - MSITSeven

Poll Name : Only Alphabets are allowed. No Empty string, please.

Group Name: CMUJ

Poll Name

ASIANQatarTrip

Poll Question

Which of these two trips would you prefer?

● Single Selection ○ Multiple Selection

# of Candidate(s)

2

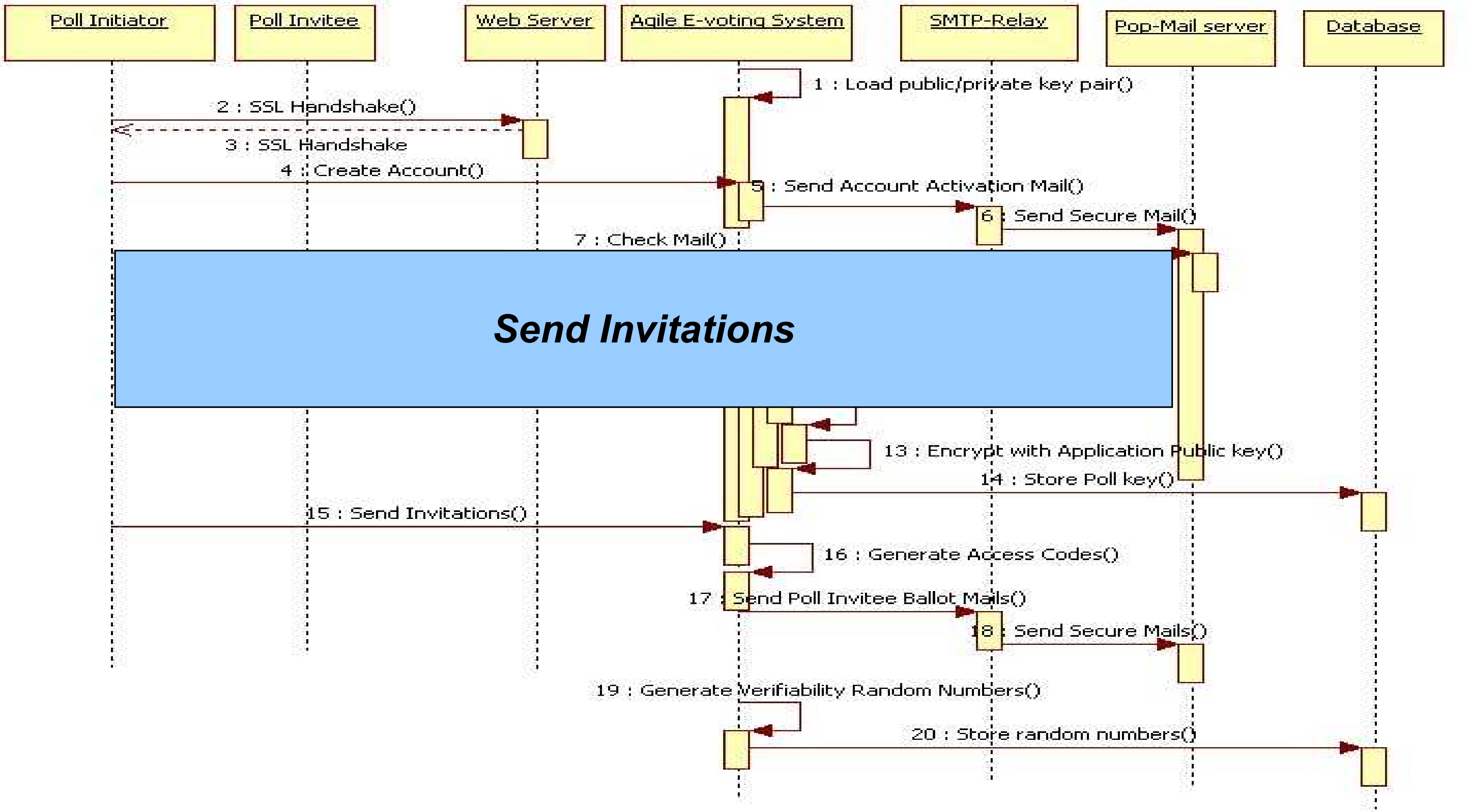
Candidate Name(s)

Desert-Safari

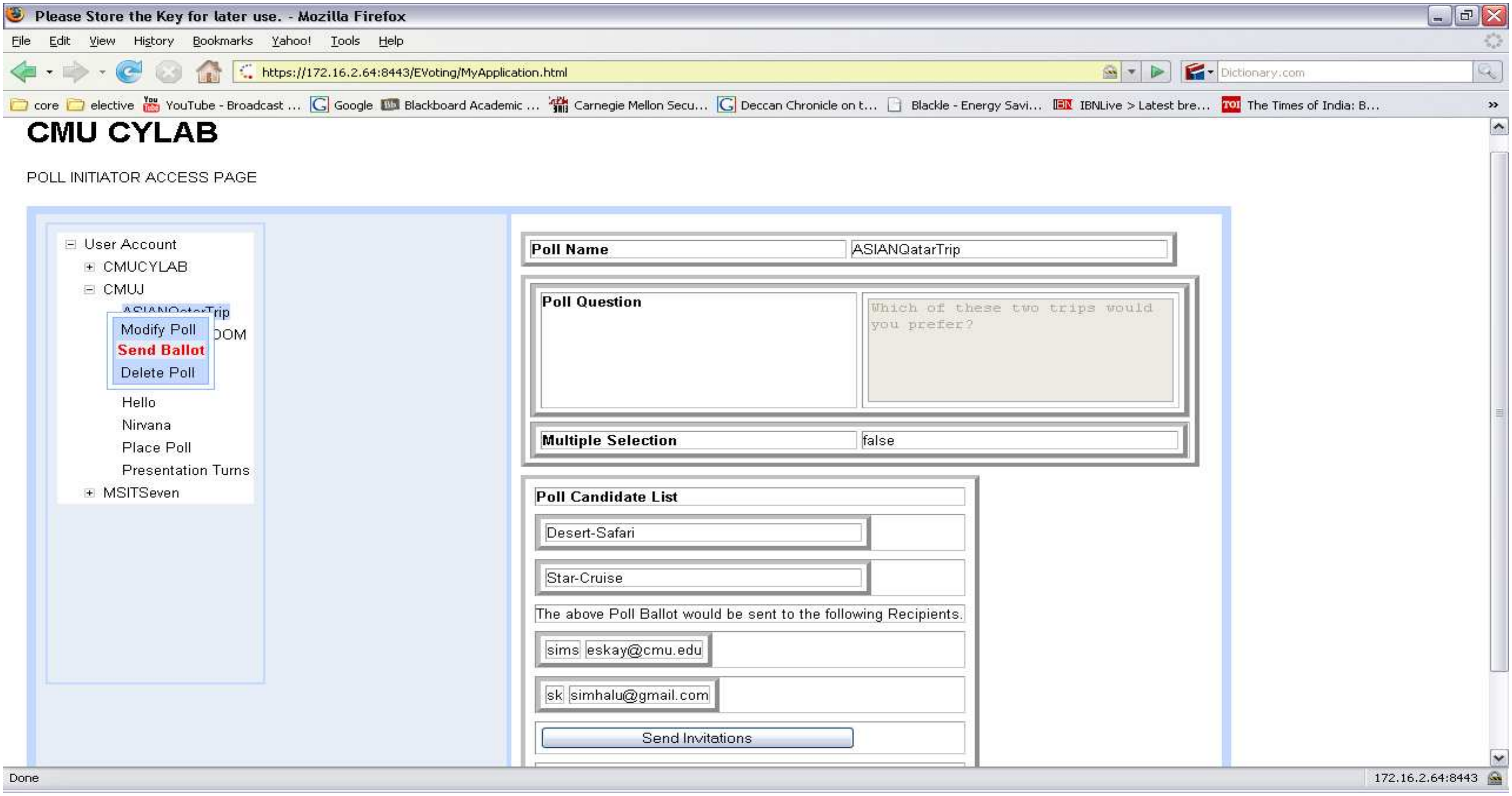
Star-Cruise

Confirm

Poll Initiator Interactions[8/9]



Poll Initiator Interactions[9/9]



CMU CYLAB

POLL INITIATOR ACCESS PAGE

- User Account
  - CMUCYLAB
  - CMUJ
    - ASIANQatarTrip
    - DOM
    - Hello
    - Nirvana
    - Place Poll
    - Presentation Turns
  - MSITSeven

Poll Name	ASIANQatarTrip
Poll Question	Which of these two trips would you prefer?
Multiple Selection	false

Poll Candidate List

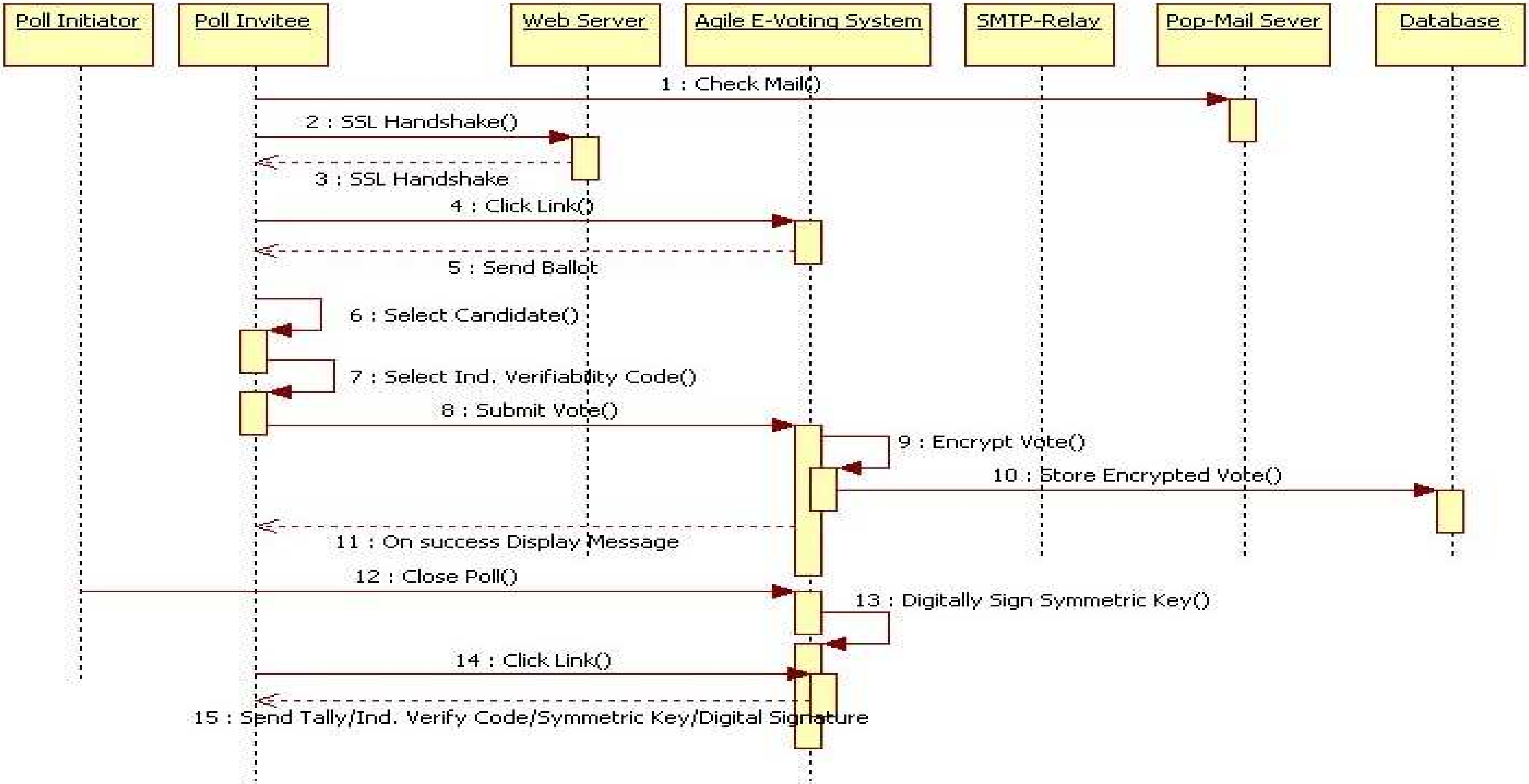
Desert-Safari

Star-Cruise

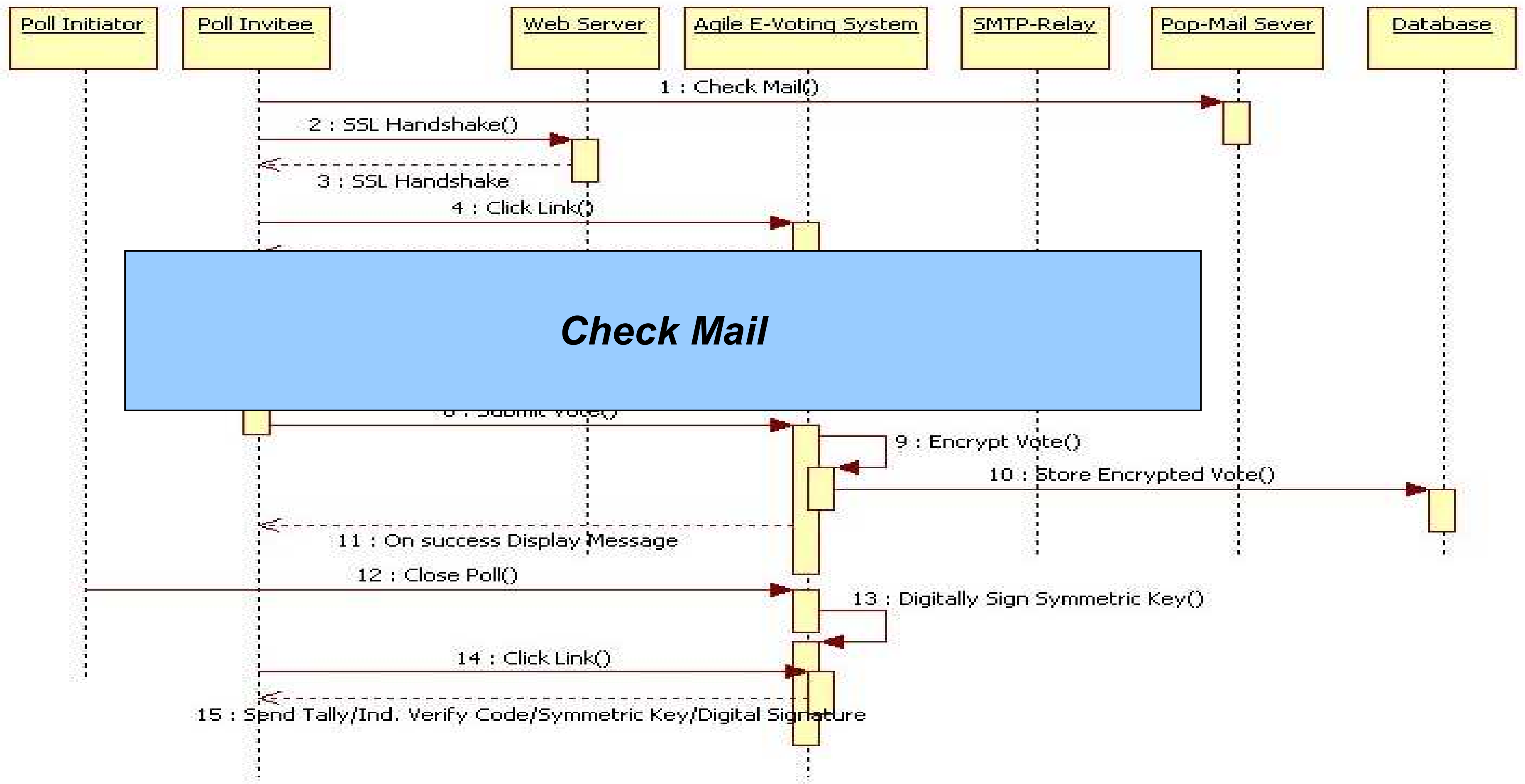
The above Poll Ballot would be sent to the following Recipients.

sims	eskay@cmu.edu
sk	simhalu@gmail.com

Poll Invitee Interactions[1/11]

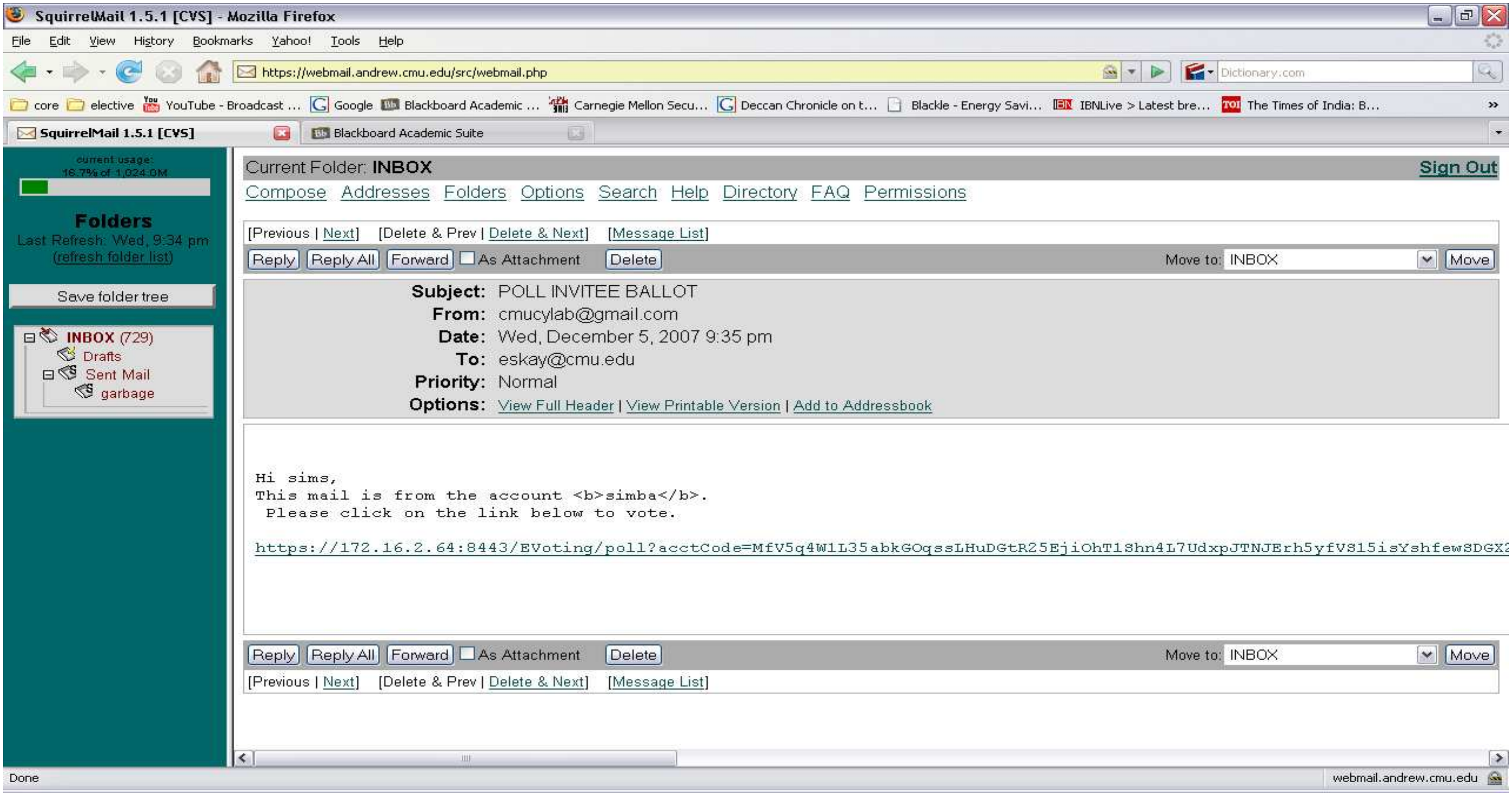


Poll Invitee Interactions[2/11]



Check Mail

Poll Invitee Interactions[3/11]

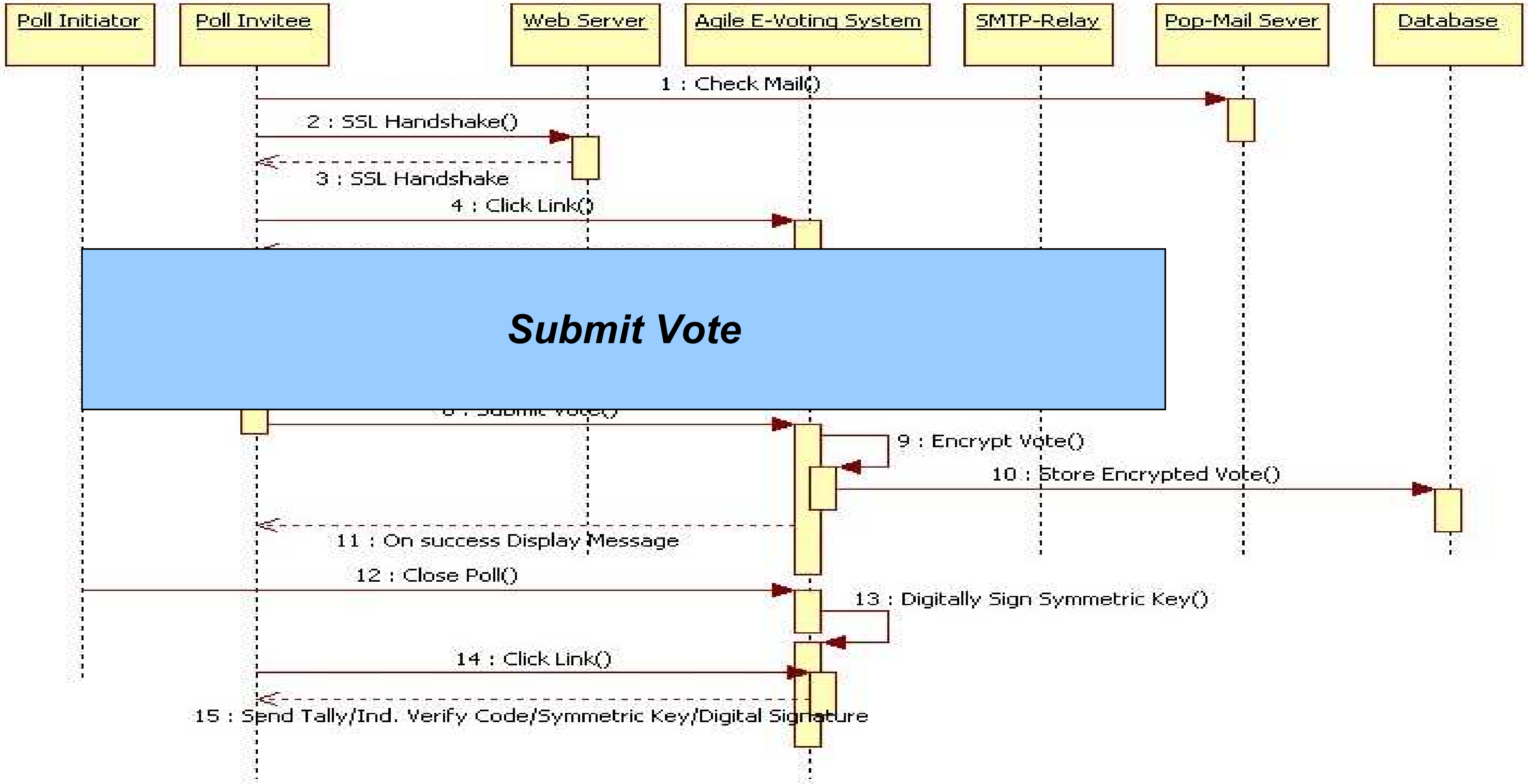

SquirrelMail 1.5.1 [CVS] - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://webmail.andrew.cmu.edu/src/webmail.php
Dictionary.com
core elective YouTube - Broadcast ... Google Blackboard Academic ... Carnegie Mellon Secu... Deccan Chronicle on t... Blackle - Energy Savi... IBNLive > Latest bre... The Times of India: B...
SquirrelMail 1.5.1 [CVS]
Blackboard Academic Suite
current usage:
16.7% of 1,024.0M
Folders
Last Refresh: Wed, 9:34 pm
(refresh folder list)
Save folder tree
INBOX (729)
Drafts
Sent Mail
garbage
Current Folder: INBOX
Sign Out
Compose Addresses Folders Options Search Help Directory FAQ Permissions
[Previous | Next] [Delete & Prev | Delete & Next] [Message List]
Reply Reply All Forward □ As Attachment Delete
Move to: INBOX Move
Options: View Full Header | View Printable Version | Add to Addressbook
Done
webmail.andrew.cmu.edu

Subject: POLL INVITEE BALLOT
From: cmucylab@gmail.com
Date: Wed, December 5, 2007 9:35 pm
To: eskay@cmu.edu
Priority: Normal

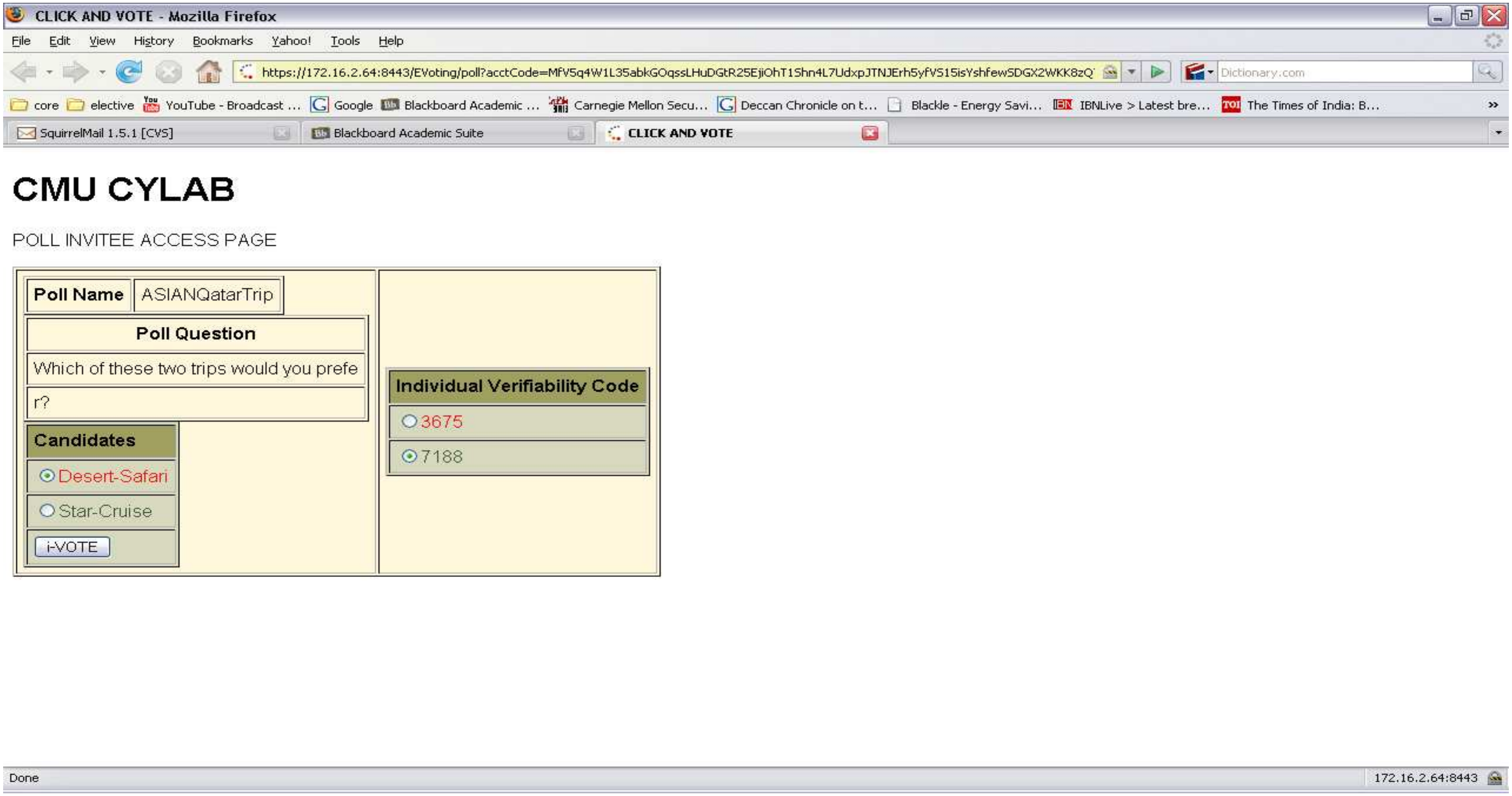
```
Hi sims,
This mail is from the account <b>simba</b>.
 Please click on the link below to vote.

https://172.16.2.64:8443/EVoting/poll?acctCode=MfV5q4W1L35abkGOqssLHuDGtR25EjiOhT1Shn4L7UdxpJTNJErh5yfVS15isYshfewSDGX
```

Poll Invitee Interactions[4/11]



Poll Invitee Interactions[5/11]



CMU CYLAB

POLL INVITEE ACCESS PAGE

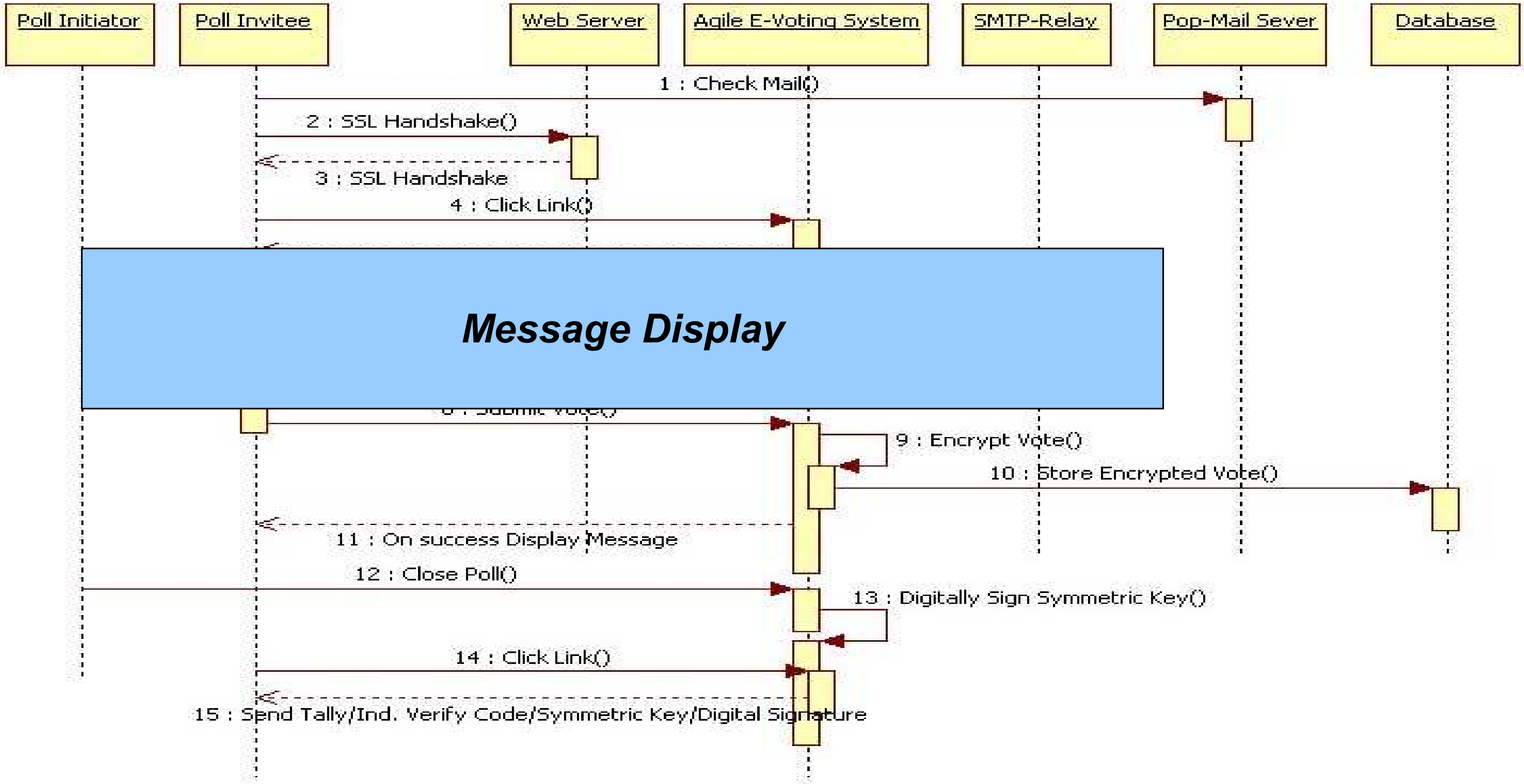
Poll Name	ASIANQatarTrip

Poll Question
Which of these two trips would you prefe
r?

Candidates
● Desert-Safari
○ Star-Cruise
i-VOTE

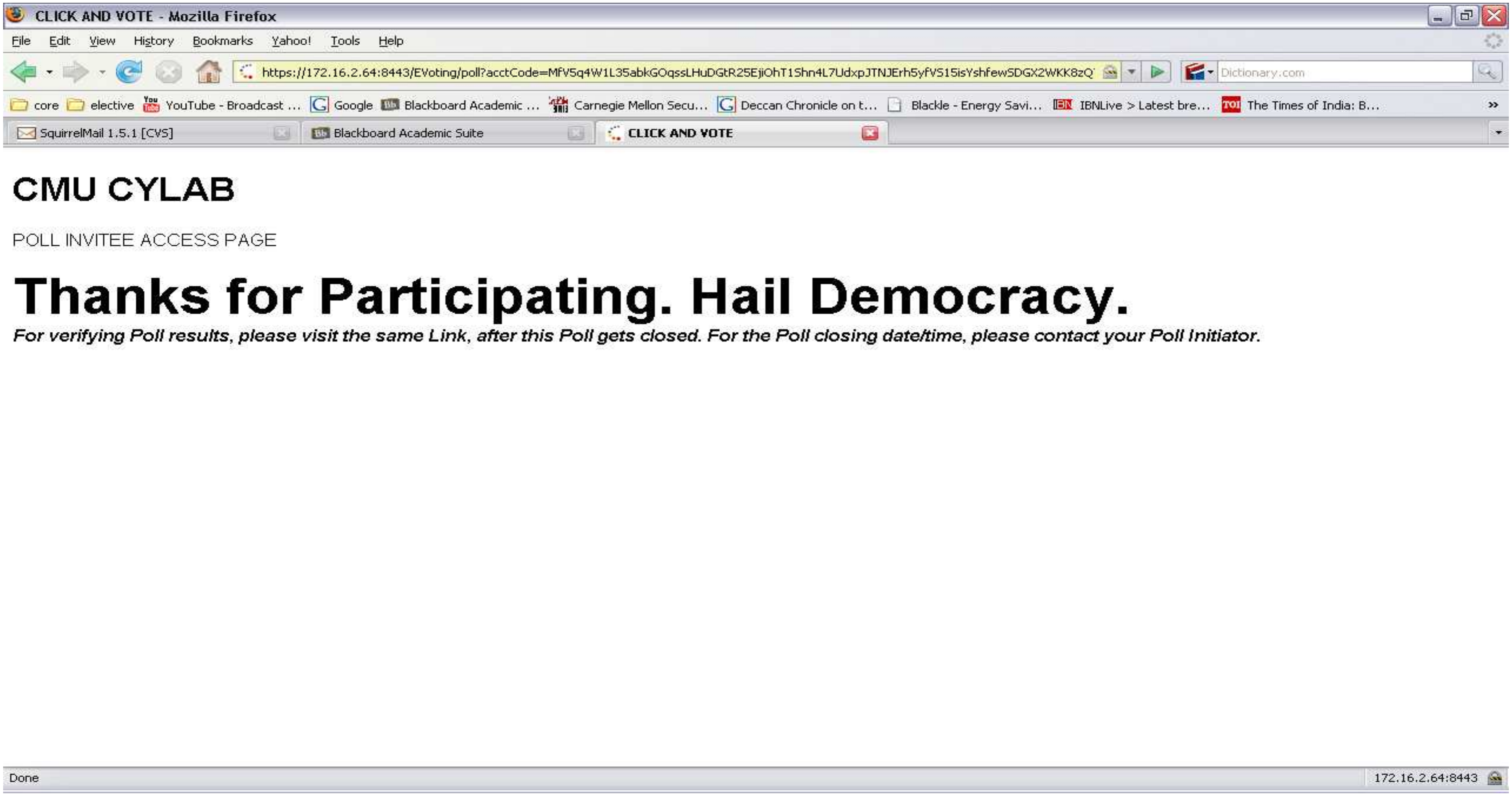
Individual Verifiability Code
○ 3675
● 7188

Poll Invitee Interactions[6/11]



Message Display

Poll Invitee Interactions[7/11]



https://172.16.2.64:8443/EVoting/poll?acctCode=MfV5q4W1L35abkGOqssLHuDGtR25EjiOhT1Shn4L7UdxpJTNJErh5yfVS15isYshfewSDGX2WKK8zQ

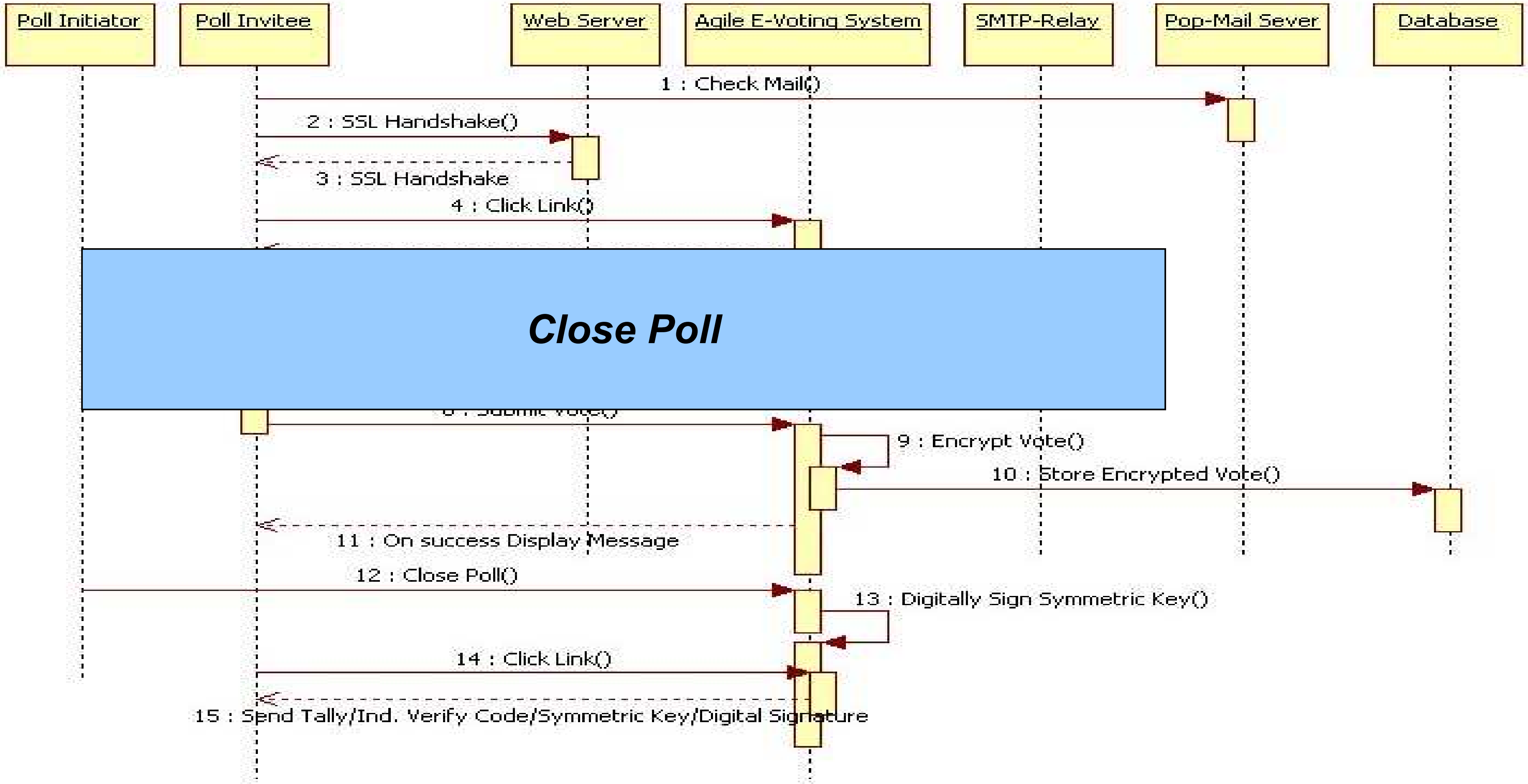
CMU CYLAB

POLL INVITEE ACCESS PAGE

Thanks for Participating. Hail Democracy.

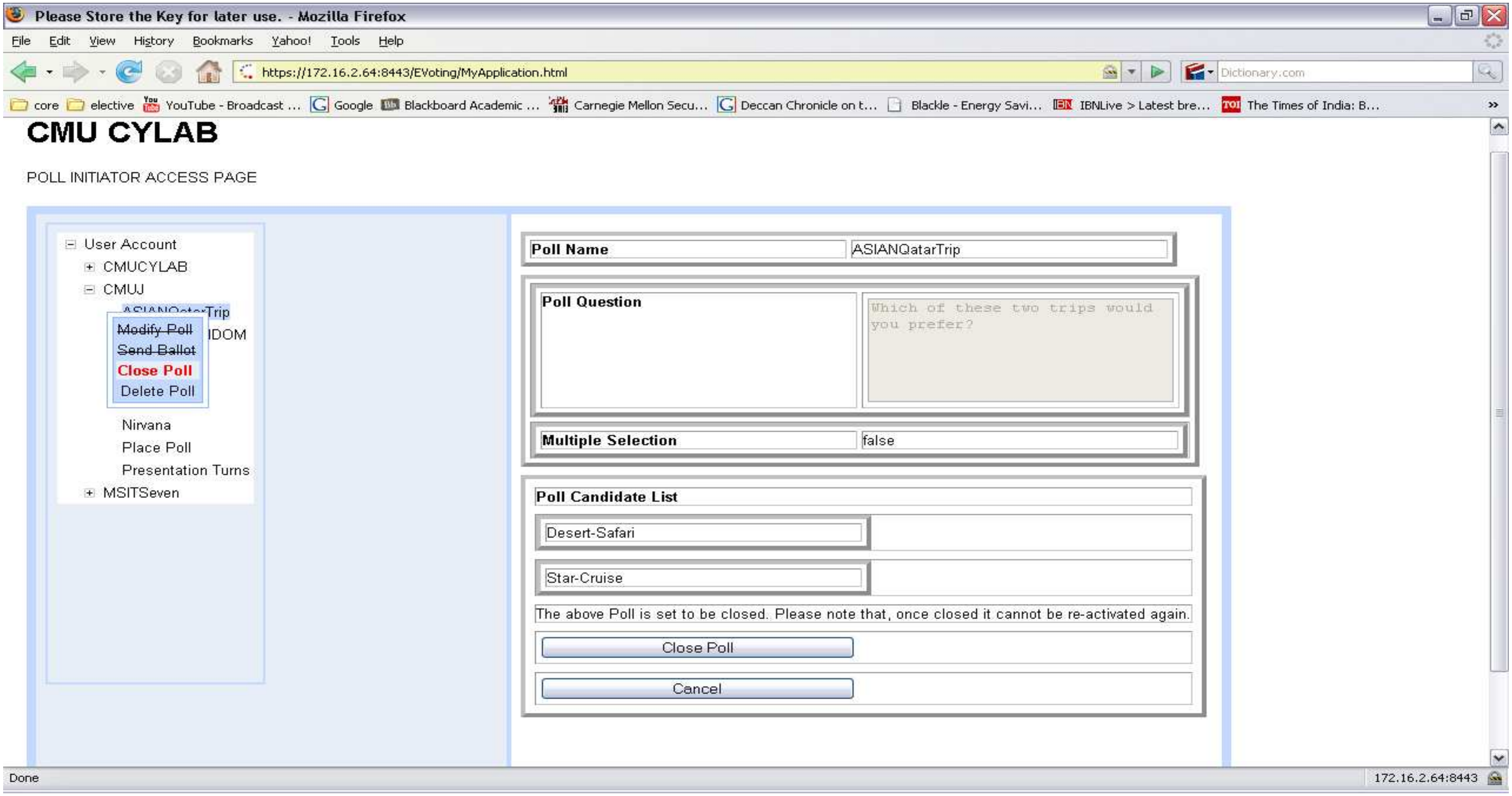
For verifying Poll results, please visit the same Link, after this Poll gets closed. For the Poll closing date/time, please contact your Poll Initiator.

Poll Invitee Interactions[8/11]



Close Poll

Poll Invitee Interactions[9/11]


Please Store the Key for later use. - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://172.16.2.64:8443/EVoting/MyApplication.html
Dictionary.com
core elective YouTube - Broadcast ... Google Blackboard Academic ... Carnegie Mellon Secu... Deccan Chronicle on t... Blackle - Energy Savi... IBNLive > Latest bre... The Times of India: B...
User Account
CMUCYLAB
CMUJ
ASIANQatarTrip
~~Modify Poll~~
~~Send Ballot~~
Close Poll
Delete Poll
IDOM
Nirvana
Place Poll
Presentation Turns
MSITSeven
Close Poll
Cancel
Done
172.16.2.64:8443

CMU CYLAB

POLL INITIATOR ACCESS PAGE

Poll Name	ASIANQatarTrip
Poll Question	Which of these two trips would you prefer?
Multiple Selection	false

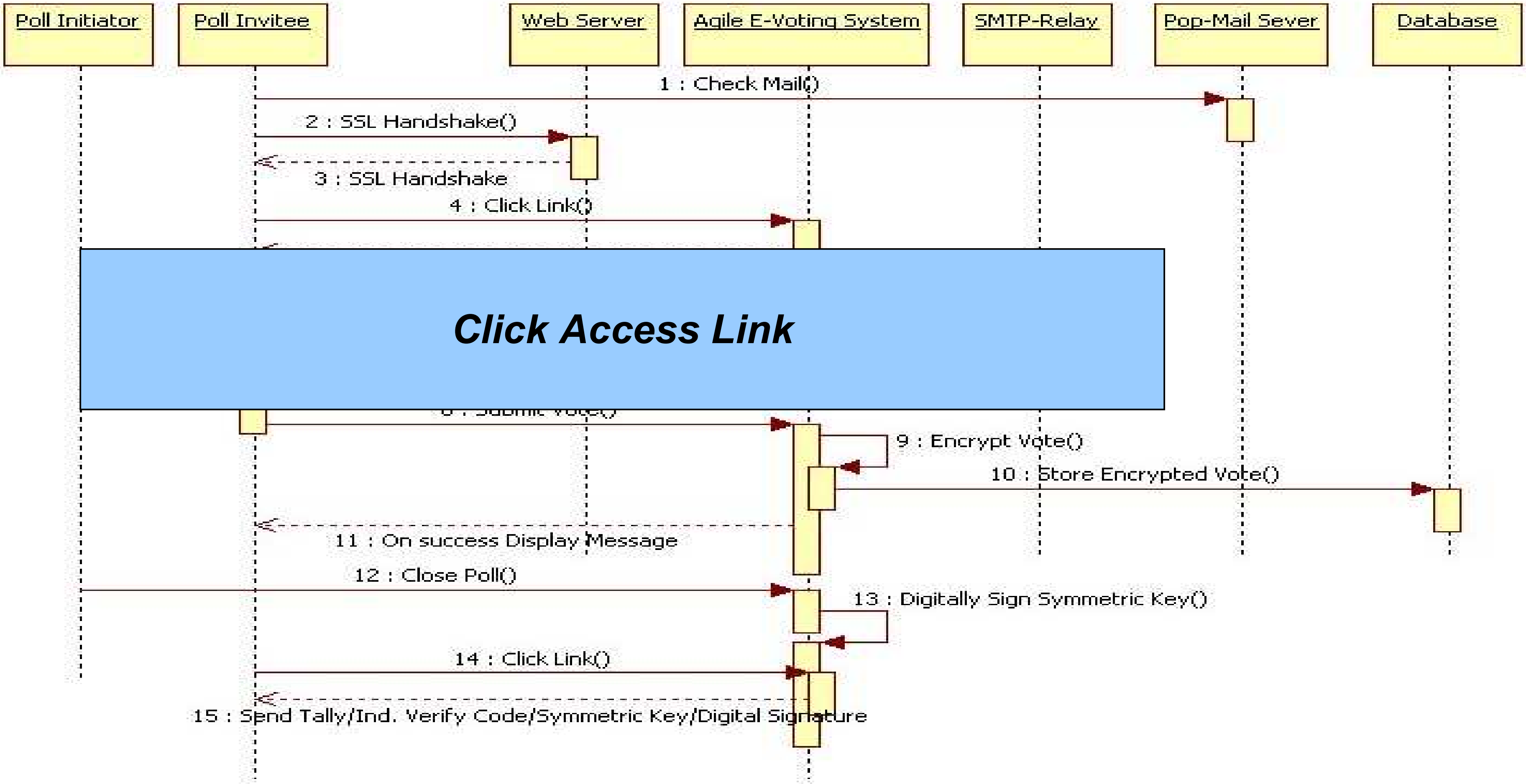
Poll Candidate List

Desert-Safari

Star-Cruise

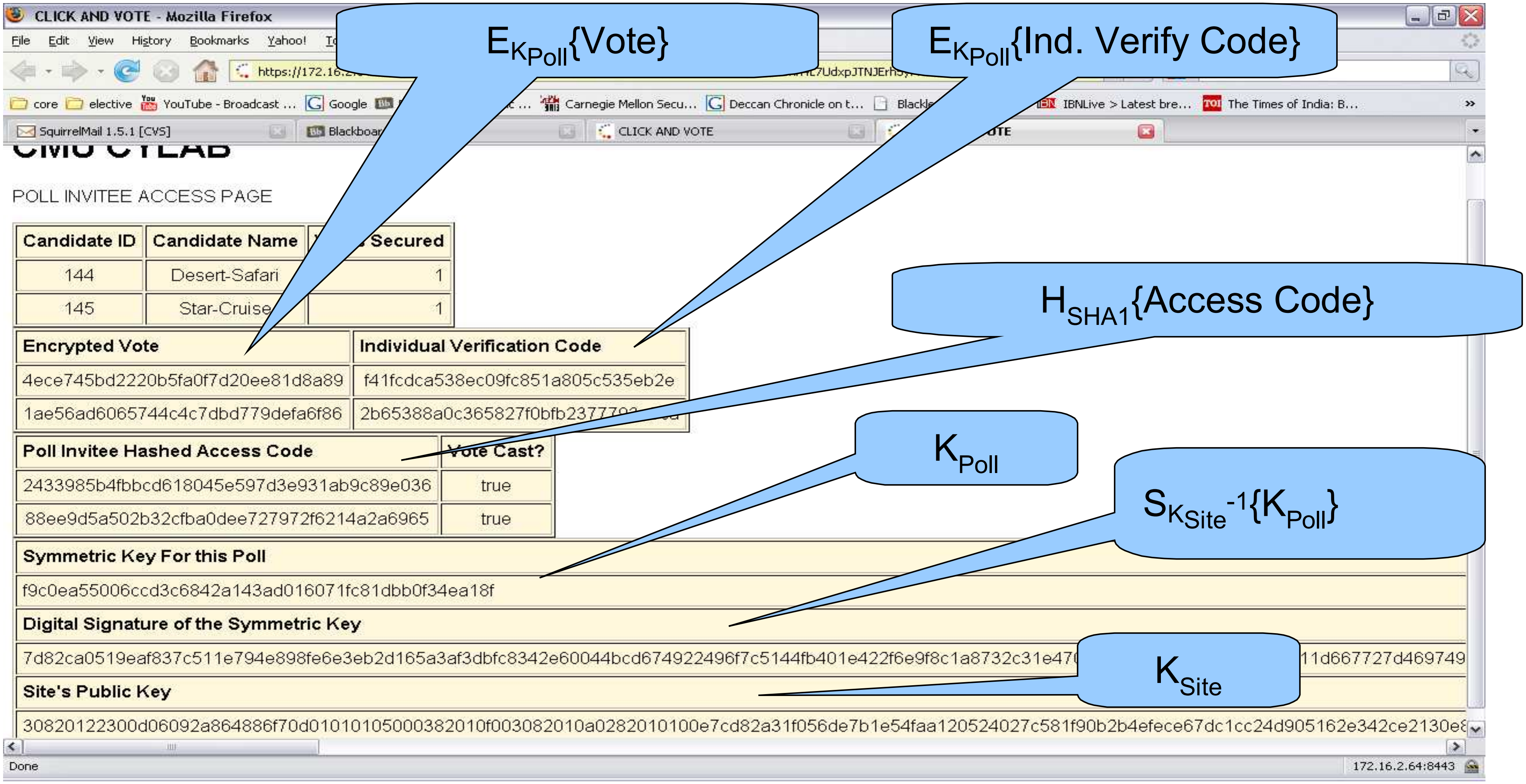
The above Poll is set to be closed. Please note that, once closed it cannot be re-activated again.

Poll Invitee Interactions[10/11]



Click Access Link

Poll Invitee Interactions[11/11]



CLICK AND VOTE - Mozilla Firefox
File Edit View History Bookmarks Yahoo!
https://172.16.2...
core elective YouTube - Broadcast ... Google Carnegie Mellon Secu... Deccan Chronicle on t... IBNLive > Latest bre... The Times of India: B...
SquirrelMail 1.5.1 [CVS] Blackboard CLICK AND VOTE
Done
172.16.2.64:8443
$E_{K_{Poll}}\{Vote\}$
$E_{K_{Poll}}\{\text{Ind. Verify Code}\}$
$H_{SHA1}\{\text{Access Code}\}$
K_{Poll}
$S_{K_{Site}^{-1}}\{K_{Poll}\}$
K_{Site}

CMU CYLAB

POLL INVITEE ACCESS PAGE

Candidate ID	Candidate Name	Votes Secured
144	Desert-Safari	1
145	Star-Cruise	1

Encrypted Vote	Individual Verification Code
4ece745bd2220b5fa0f7d20ee81d8a89	f41fcdca538ec09fc851a805c535eb2e
1ae56ad6065744c4c7dbd779defa6f86	2b65388a0c365827f0bfb2377792

Poll Invitee Hashed Access Code	Vote Cast?
2433985b4fbbcd618045e597d3e931ab9c89e036	true
88ee9d5a502b32cfba0dee727972f6214a2a6965	true

Symmetric Key For this Poll

f9c0ea55006ccd3c6842a143ad016071fc81dbb0f34ea18f

Digital Signature of the Symmetric Key

7d82ca0519eaf837c511e794e898fe6e3eb2d165a3af3dbfc8342e60044bcd674922496f7c5144fb401e422f6e9f8c1a8732c31e47 11d667727d469749

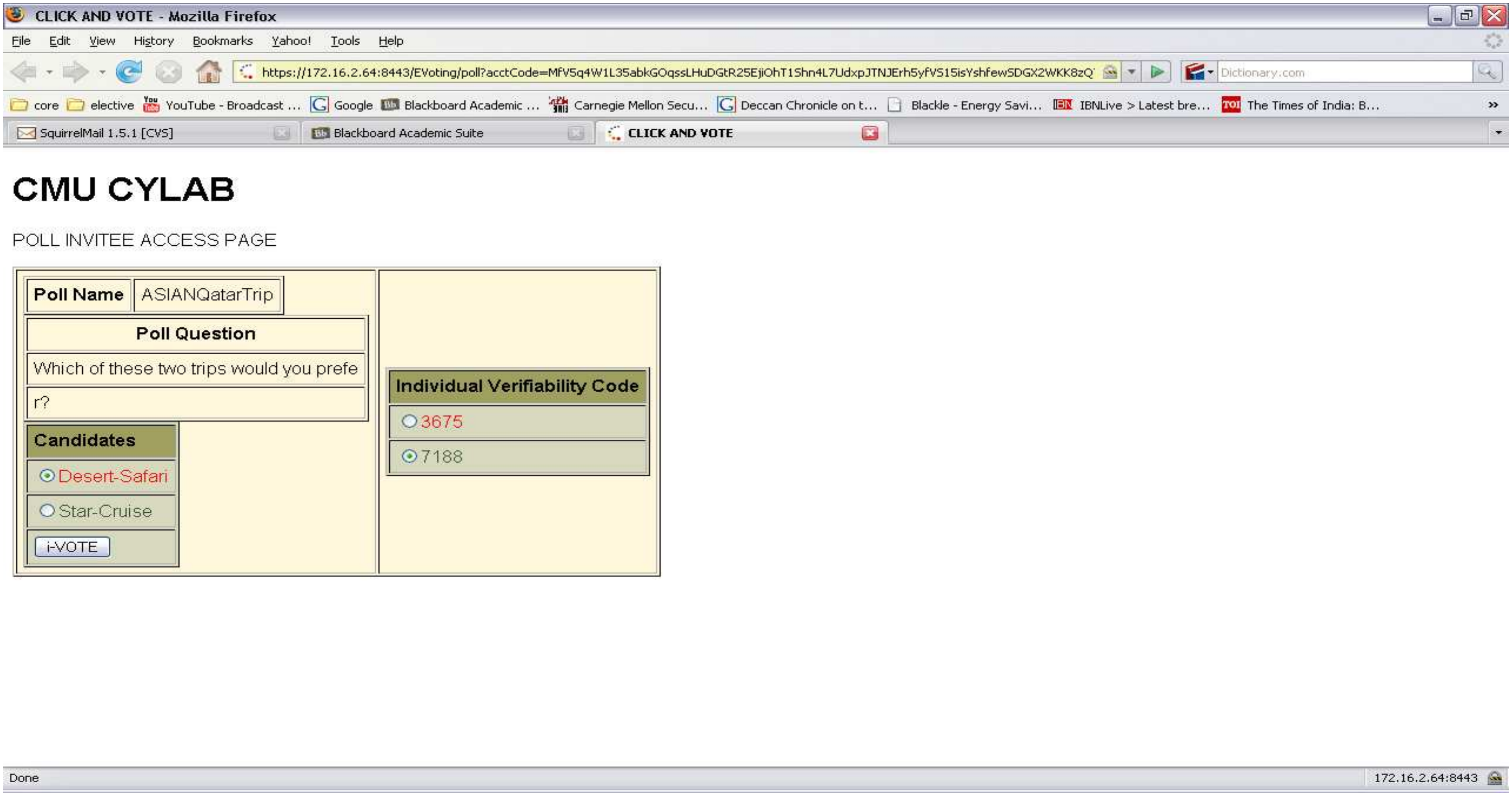
Site's Public Key

30820122300d06092a864886f70d01010105000382010f003082010a0282010100e7cd82a31f056de7b1e54faa120524027c581f90b2b4efece67dc1cc24d905162e342ce2130e

Individual Verifiability[1/3]

- Additional Random Number selection
- # of random numbers to generate N +(P-1)
- N is the Number of Invitees
- P is the size of the set of random numbers to display for each Poll Invitee

Individual Verifiability[2/3]



CMU CYLAB

POLL INVITEE ACCESS PAGE

Poll Name	ASIANQatarTrip

Poll Question

Which of these two trips would you prefe
r?

Candidates

● Desert-Safari

○ Star-Cruise

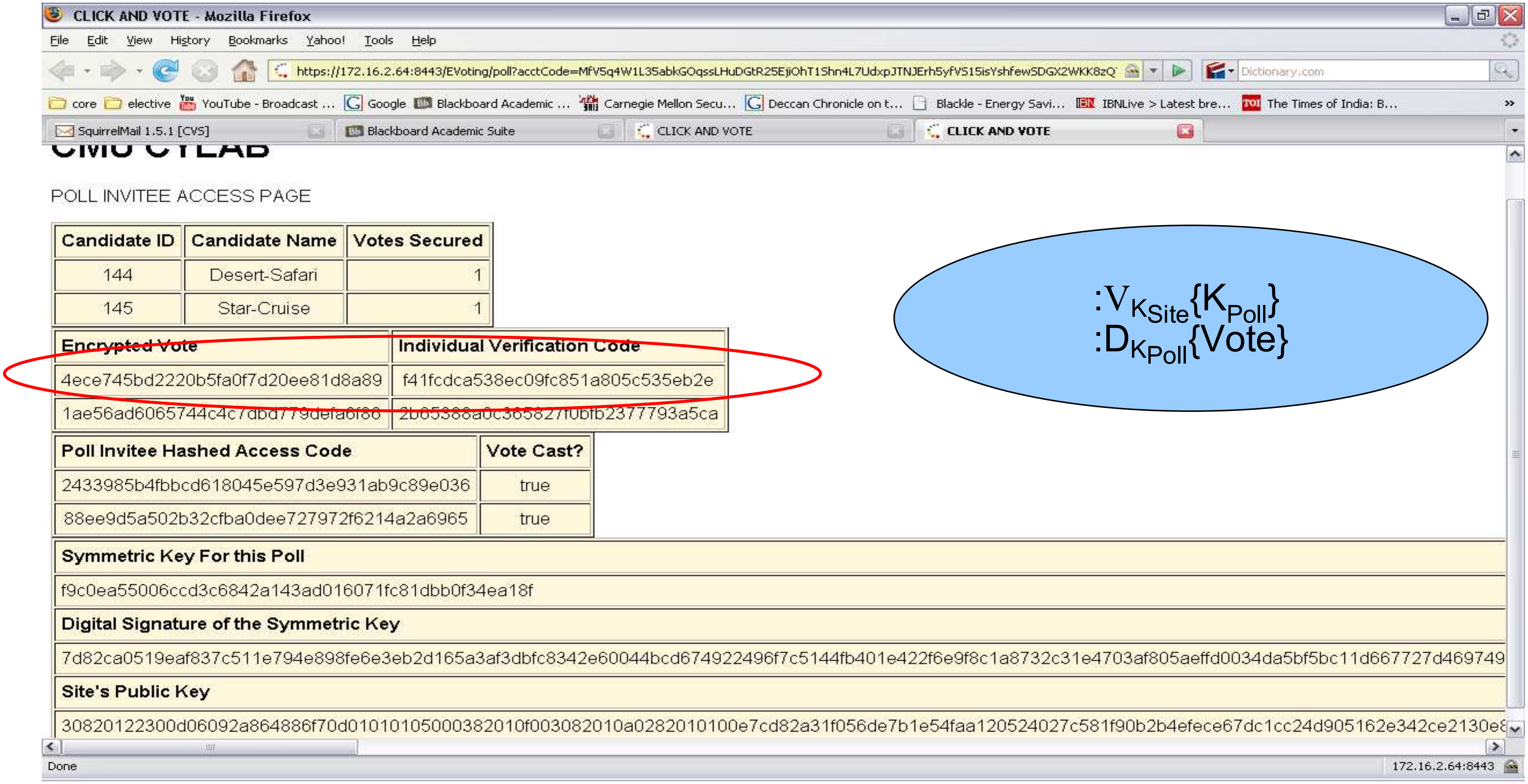
i-VOTE

Individual Verifiability Code

○ 3675

● 7188

Individual Verifiability[3/3]



CMU CYLAB

POLL INVITEE ACCESS PAGE

Candidate ID	Candidate Name	Votes Secured
144	Desert-Safari	1
145	Star-Cruise	1

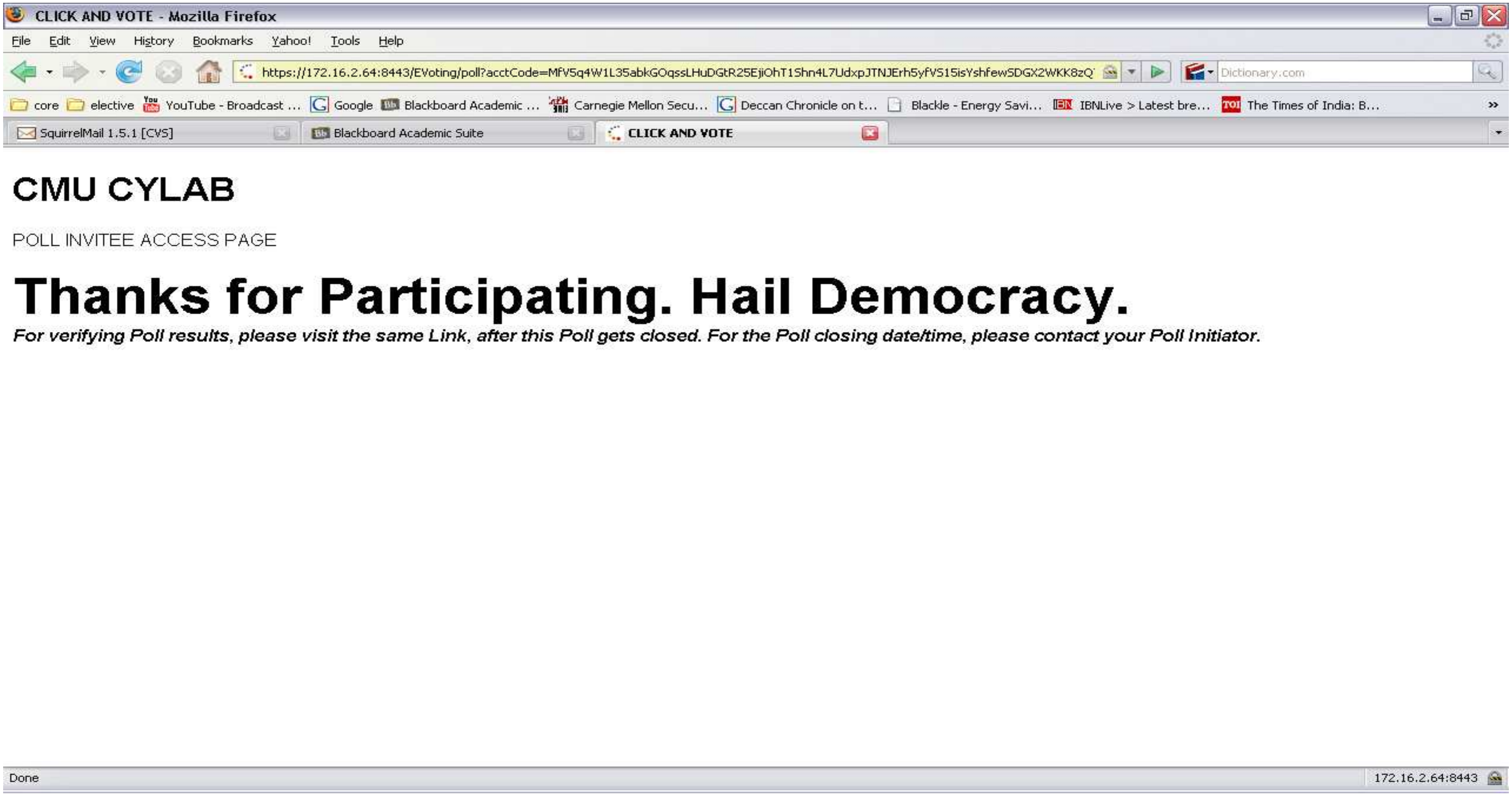
Encrypted Vote	Individual Verification Code
4ece745bd2220b5fa0f7d20ee81d8a89	f41fcdca538ec09fc851a805c535eb2e
1ae56ad6065744c4c7dbd779defa6f86	2b65388a0c365827f0bfb2377793a5ca

Poll Invitee Hashed Access Code	Vote Cast?
2433985b4fbbcd618045e597d3e931ab9c89e036	true
88ee9d5a502b32cfba0dee727972f6214a2a6965	true

Symmetric Key For this Poll
f9c0ea55006ccd3c6842a143ad016071fc81dbb0f34ea18f
Digital Signature of the Symmetric Key
7d82ca0519eaf837c511e794e898fe6e3eb2d165a3af3dbfc8342e60044bcd674922496f7c5144fb401e422f6e9f8c1a8732c31e4703af805aeffd0034da5bf5bc11d667727d469749
Site's Public Key
30820122300d06092a864886f70d01010105000382010f003082010a0282010100e7cd82a31f056de7b1e54faa120524027c581f90b2b4efece67dc1cc24d905162e342ce2130e8

$:V_{K_{Site}}\{K_{Poll}\}$
$:D_{K_{Poll}}\{Vote\}$

Receipt- Freeness



https://172.16.2.64:8443/EVoting/poll?acctCode=MfV5q4W1L35abkGOqssLHuDGtR25EjiOhT1Shn4L7UdxpJTNJErh5yfVS15isYshfewSDGX2WKK8zQ

CMU CYLAB

POLL INVITEE ACCESS PAGE

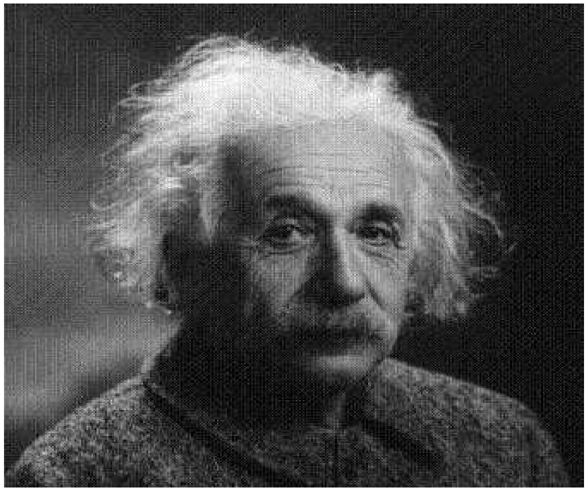
Thanks for Participating. Hail Democracy.

For verifying Poll results, please visit the same Link, after this Poll gets closed. For the Poll closing date/time, please contact your Poll Initiator.

Conclusion

- →Agility in EVoting
- →Individual Verifiability & Receipt Freeness
- →In-coercibility - the logical next step

Q & A



"Any intelligent fool can make things bigger, more complex, and more violent. It takes a touch of genius -- and a lot of courage -- to move in the opposite direction."

-- Albert Einstein