

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.
Delegates of several States shall be sufficient for the Establishment of this Constitution. In witness whereof the Delegates of the States, in Convention assembled, have signed their Names, and the Approbation of the People of the States, has been given, in the Year of our Lord one thousand seven hundred and eighty seven, and of the Independence of the United States of America the Twentieth.

Delegates

Delaware	George Read Richard Bassett Jacob Collings
Massachusetts	John Hancock
New York	John Jay Alexander Hamilton John Adams
Virginia	George Mason James Madison
North Carolina	Wm. Hooper Richard Dobson Spaight H. Williams
South Carolina	J. Rutledge Charles Cotesworth Pinckney Charles Pinckney John Rutledge
Georgia	William Few Abner Nash
New Jersey	Richard Stockton John Witherspoon George Taylor Moses Willson
New Hampshire	John Langdon Nicholas Cooke
Connecticut	Nathaniel Gorham Rufus King Samuel Elwell
Pennsylvania	Robert Morris George Ross Benjamin Franklin Thomas Mifflin James Wilson



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

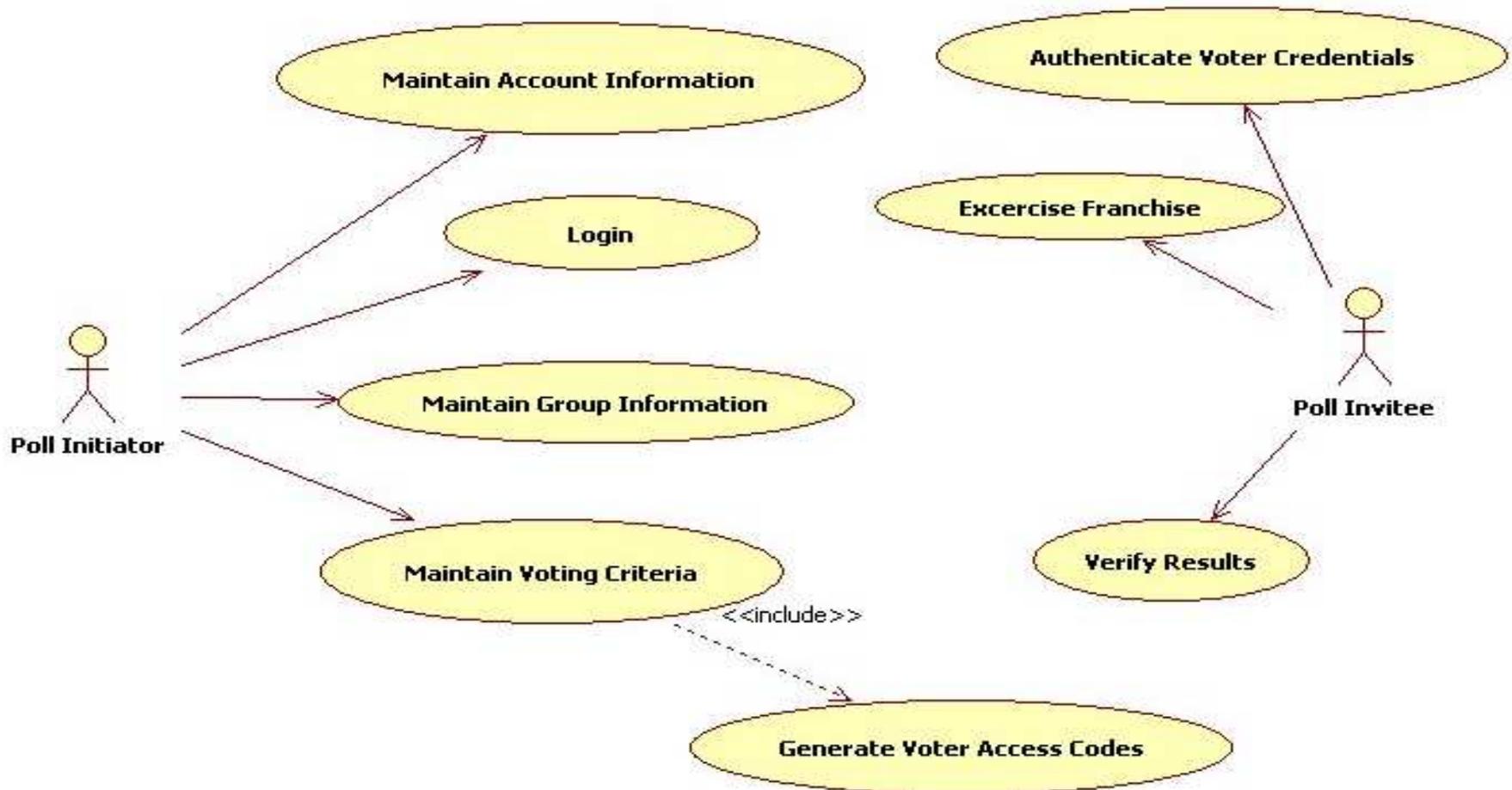
The KOA system is the first Free Software Internet voting system developed, which was used for a government election.

[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)]

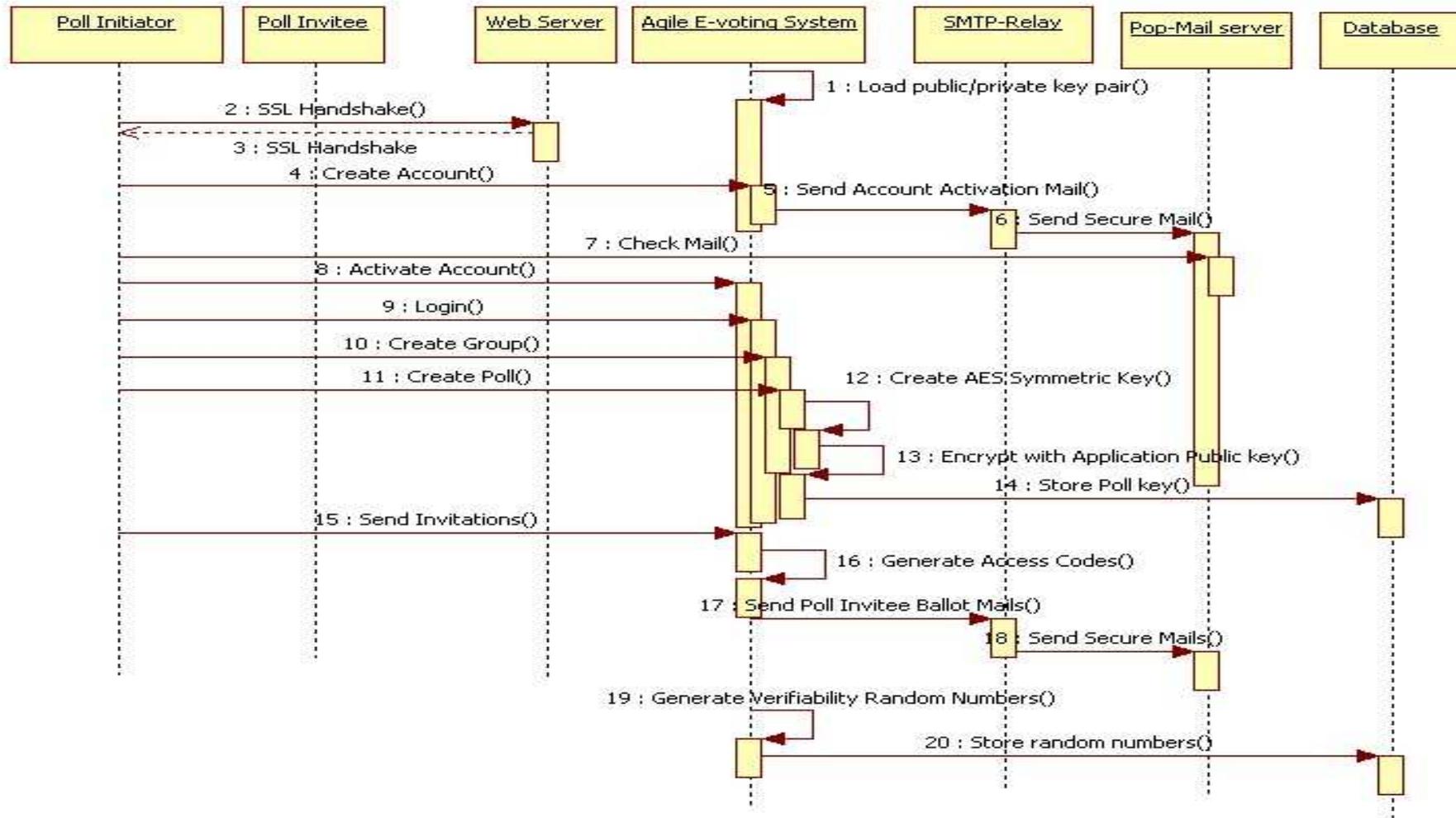
Project Overview-*The Agile Way*

- 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

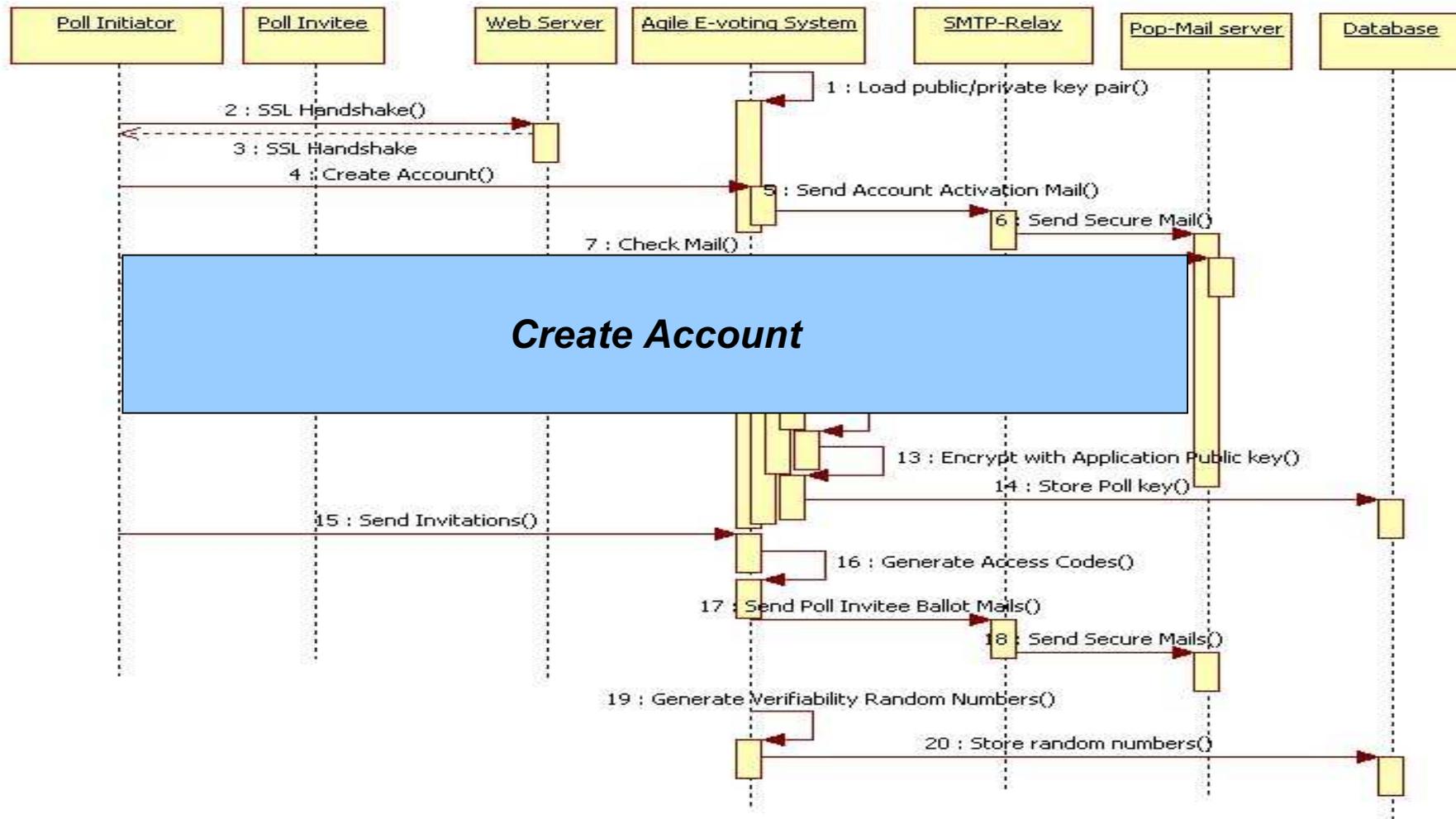
Overview – Use Case



Poll Initiator Interactions[1/9]



Poll Initiator Interactions[2/9]



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...

CMU CYLAB

POLL INITIATOR ACCESS PAGE

User ID

Password

Login

Create Account

Email: Please check the email format.

User ID

Password

Confirm Password

First Name

Last Name

E-Mail

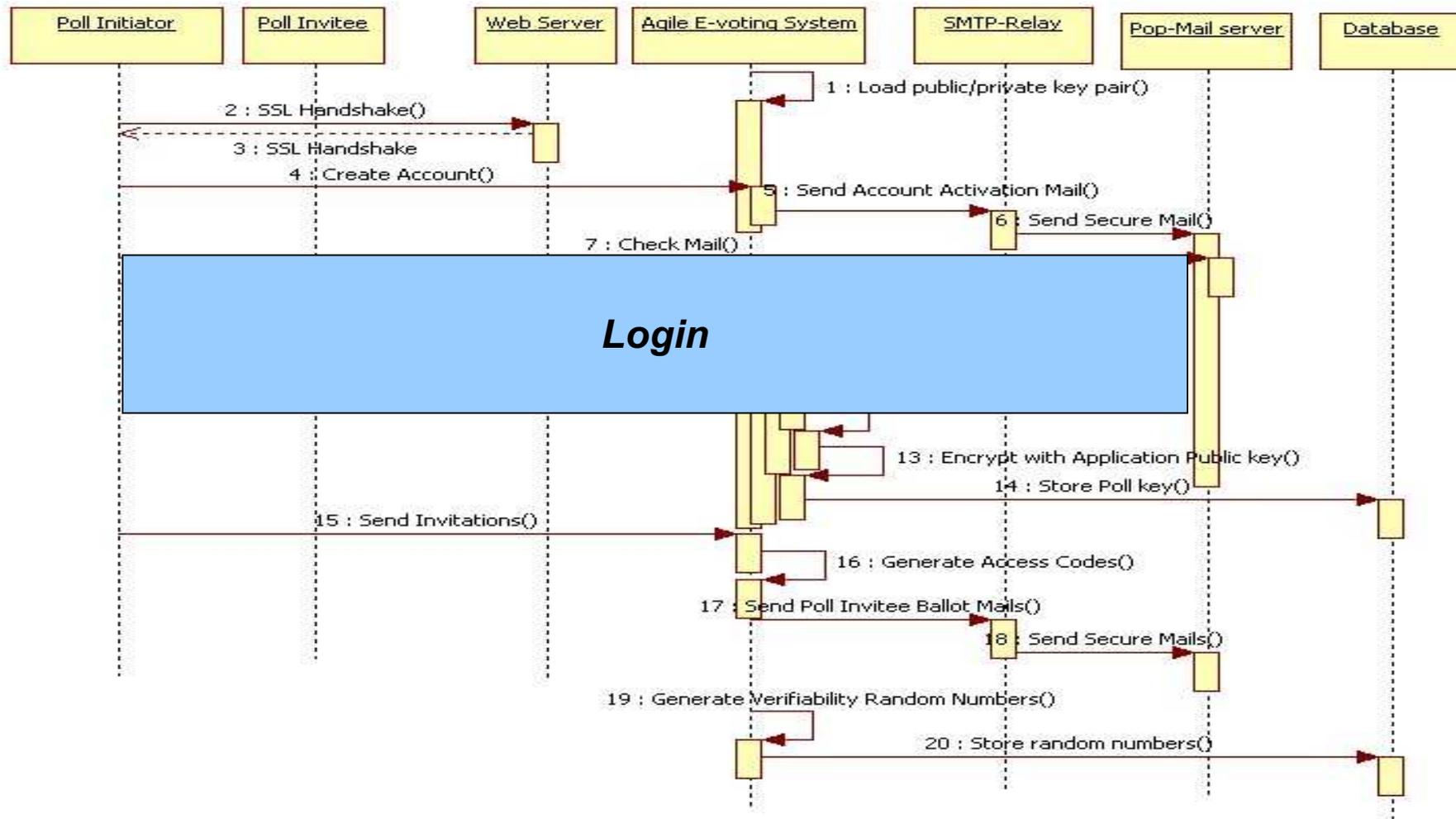
Account Activation mail would be sent to the e-mail address entered above.

What is your pet's name?

Submit Cancel

Done 172.16.2.64:8443

Poll Initiator Interactions[4/9]



Poll Initiator Interactions[5/9]

The screenshot shows a Mozilla Firefox browser window titled "CMU CYLAB - Mozilla Firefox". The address bar displays the URL "https://172.16.2.64:8443/EVoting/MyApplication.html". The browser's menu bar includes "File", "Edit", "View", "History", "Bookmarks", "Yahoo!", "Tools", and "Help". The address bar also shows a search engine icon and the text "Dictionary.com". The browser's tab bar shows several open tabs, including "core", "elective", "YouTube - Broadcast ...", "Google", "Blackboard Academic ...", "Carnegie Mellon Secu...", "Deccan Chronicle on t...", "Blackle - Energy Savi...", "IBNLive > Latest bre...", and "The Times of India: B...".

The main content area of the browser displays the "CMU CYLAB" logo and the text "POLL INITIATOR ACCESS PAGE". Below this, there is a sidebar on the left with a "User Account" menu containing the following items:

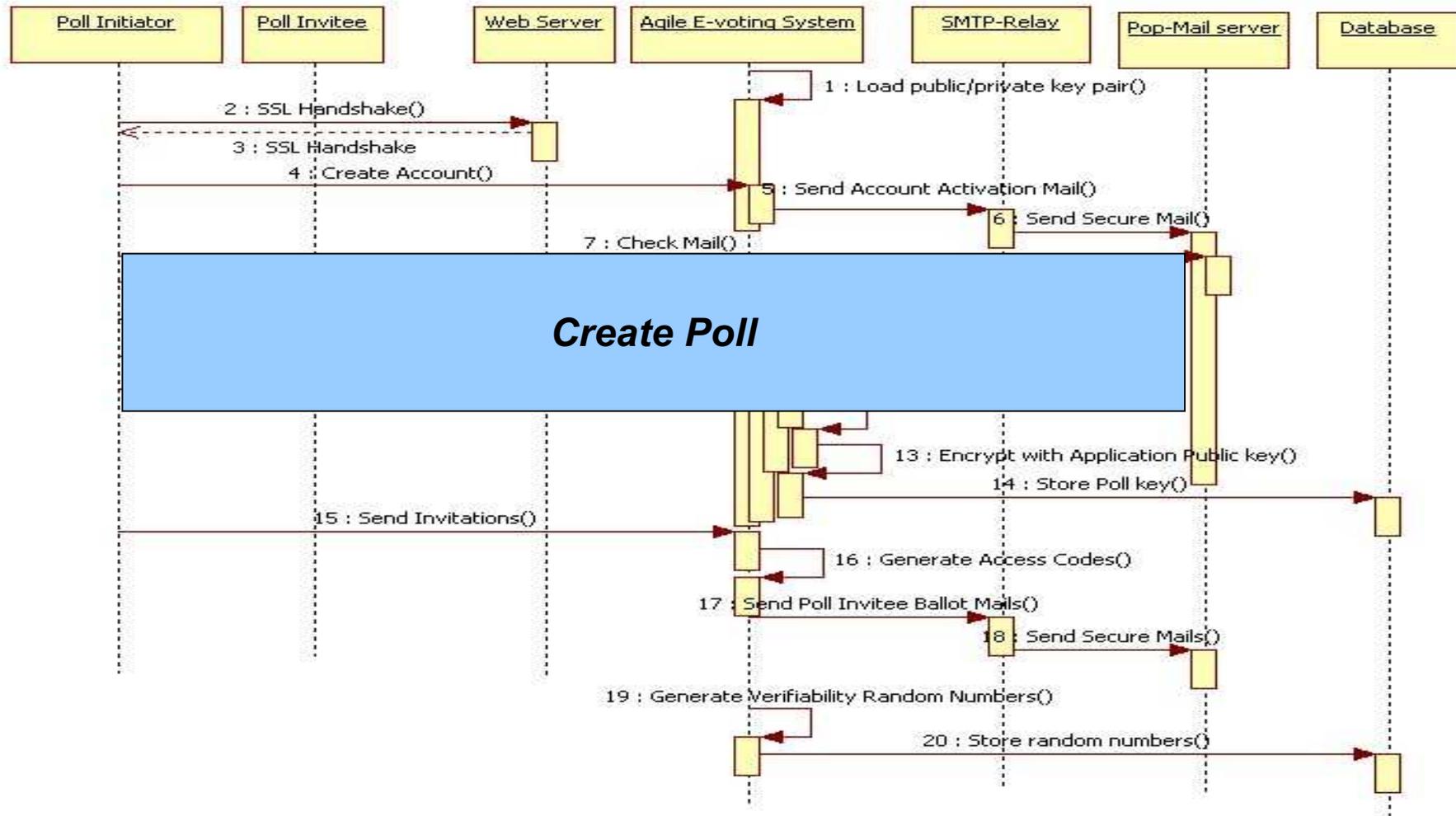
- User Account
 - CMUCYLAB
 - CMUJ
 - MSITSeven

The main content area contains a form with four input fields, each with a label and a value:

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

The browser's status bar at the bottom shows "Done" on the left and "172.16.2.64:8443" on the right.

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...

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

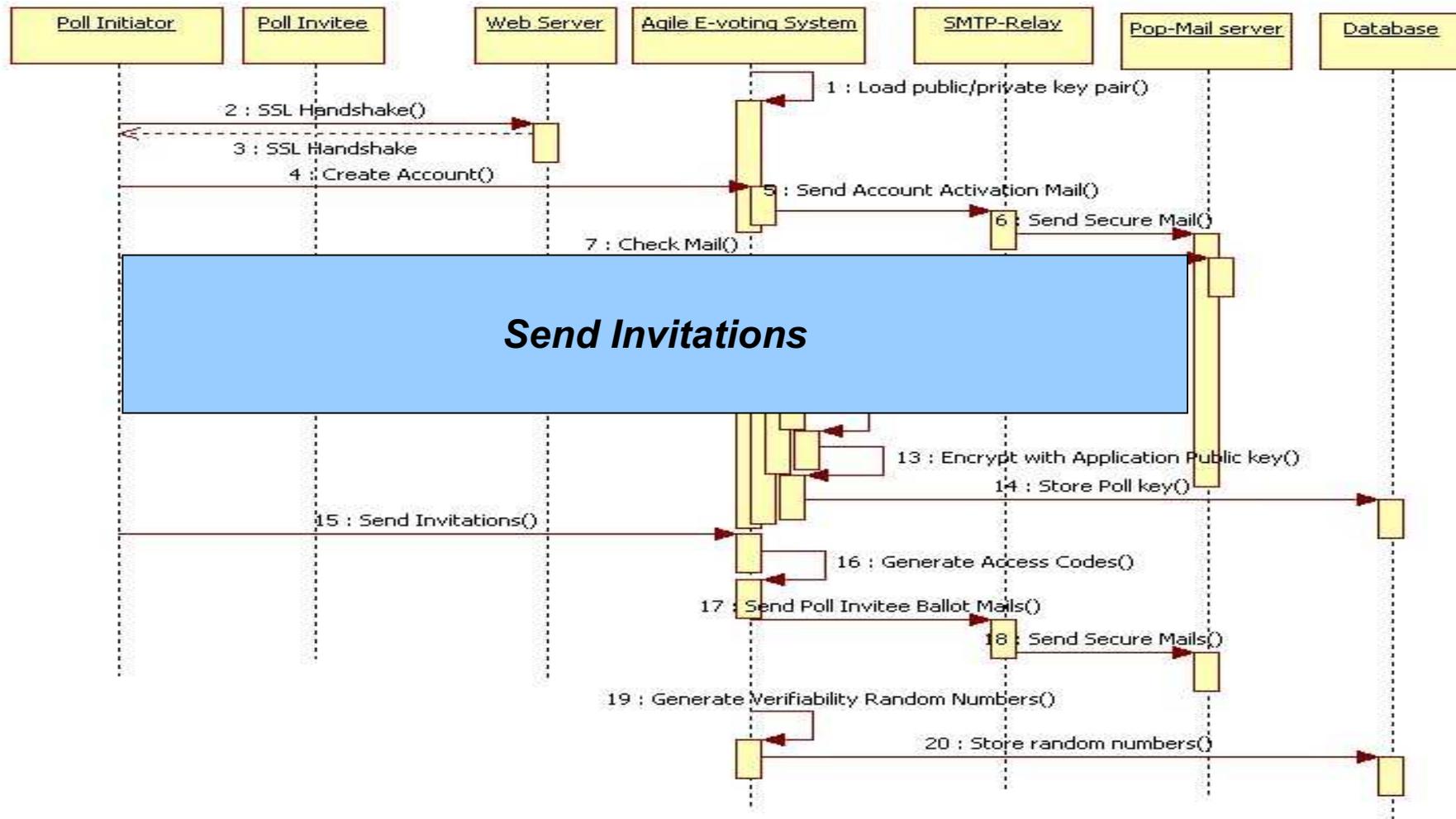
Candidate Name(s):

- Desert-Safari
- Star-Cruise

Confirm

Done 172.16.2.64:8443

Poll Initiator Interactions[8/9]



Poll Initiator Interactions[9/9]

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...

CMU CYLAB

POLL INITIATOR ACCESS PAGE

- User Account
 - CMUCYLAB
 - CMUJ
 - ASIANQatarTrip
 - Modify Poll
 - Send Ballot**
 - Delete Poll
 - 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

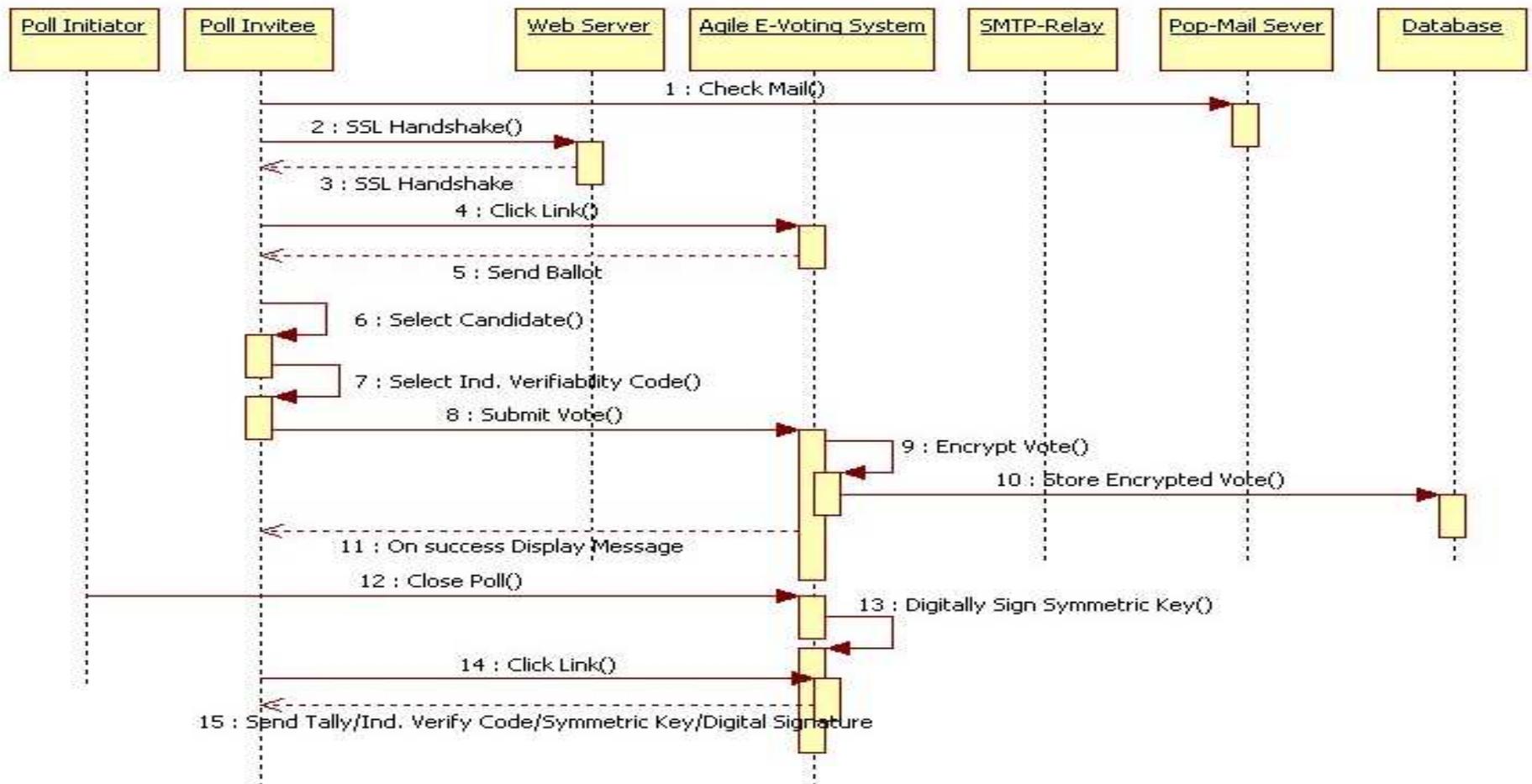
The above Poll Ballot would be sent to the following Recipients.

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

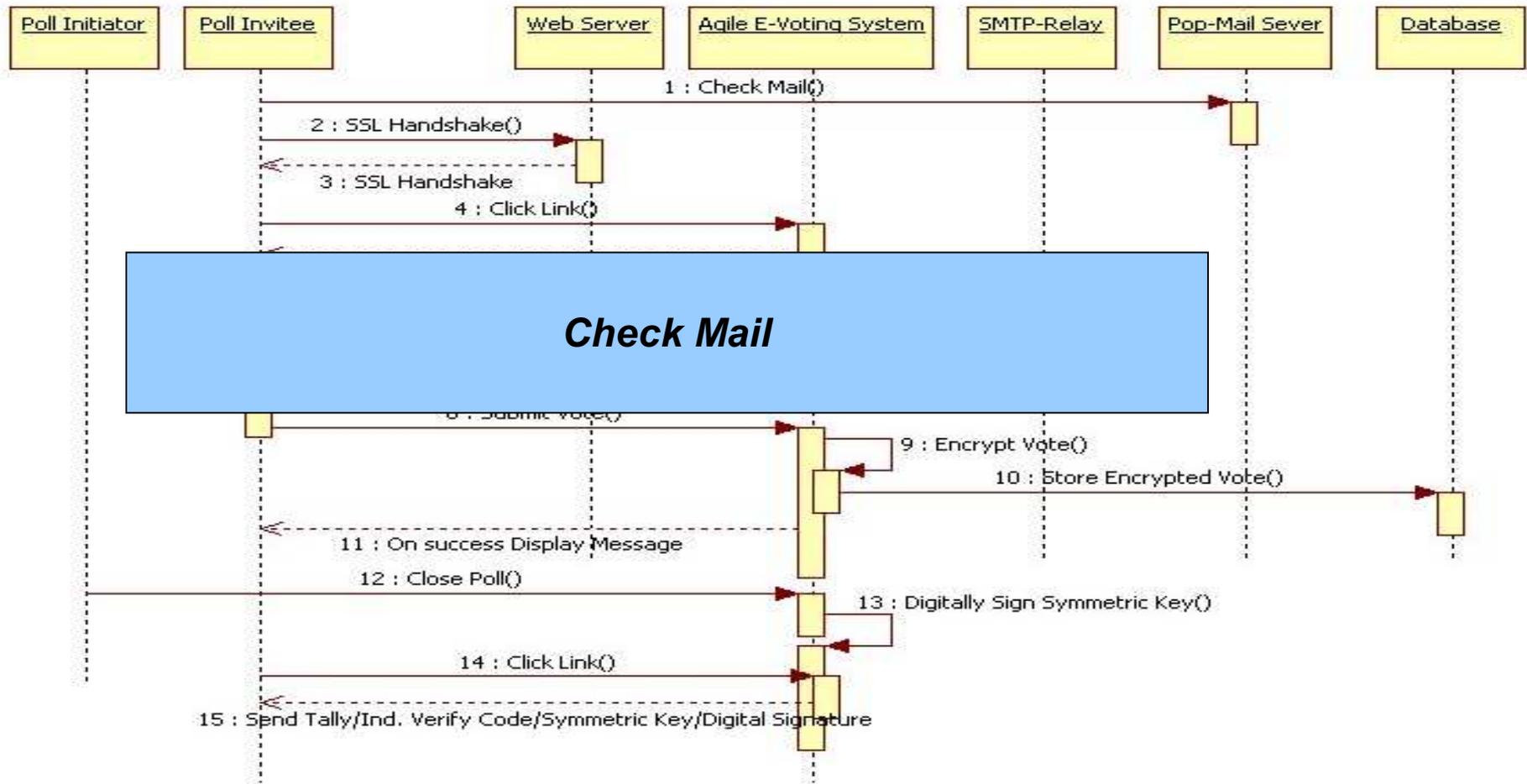
Send Invitations

Done 172.16.2.64:8443

Poll Invitee Interactions[1/11]



Poll Invitee Interactions[2/11]



Poll Invitee Interactions[3/11]

The screenshot shows the SquirrelMail 1.5.1 interface within a Mozilla Firefox browser window. The browser's address bar displays the URL `https://webmail.andrew.cmu.edu/src/webmail.php`. The interface includes a menu bar (File, Edit, View, History, Bookmarks, Yahoo!, Tools, Help) and a toolbar with navigation icons. The main content area is titled "Current Folder: INBOX" and features a "Sign Out" link. Below this, there are navigation links: "Compose", "Addresses", "Folders", "Options", "Search", "Help", "Directory", "FAQ", and "Permissions". A secondary navigation bar contains "[Previous | Next]", "[Delete & Prev | Delete & Next]", and "[Message List]". The email header section includes buttons for "Reply", "Reply All", "Forward", "As Attachment", and "Delete", along with a "Move to: INBOX" dropdown menu and a "Move" button. The email details are as follows:

- Subject:** POLL INVITEE BALLOT
- From:** cmucylab@gmail.com
- Date:** Wed, December 5, 2007 9:35 pm
- To:** eskay@cmu.edu
- Priority:** Normal
- Options:** [View Full Header](#) | [View Printable Version](#) | [Add to Addressbook](#)

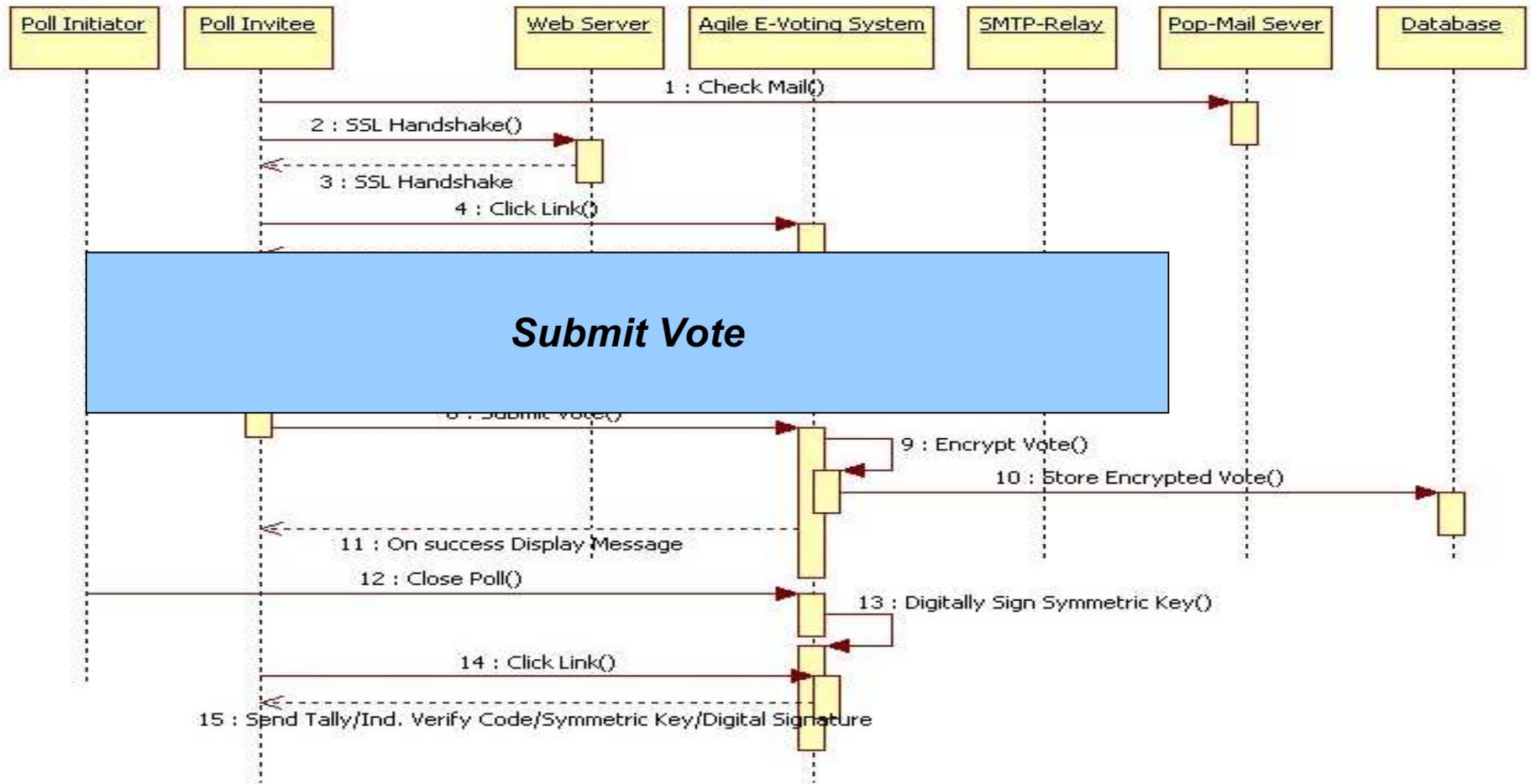
The email body contains the following text:

Hi sims,
This mail is from the account simba.
Please click on the link below to vote.

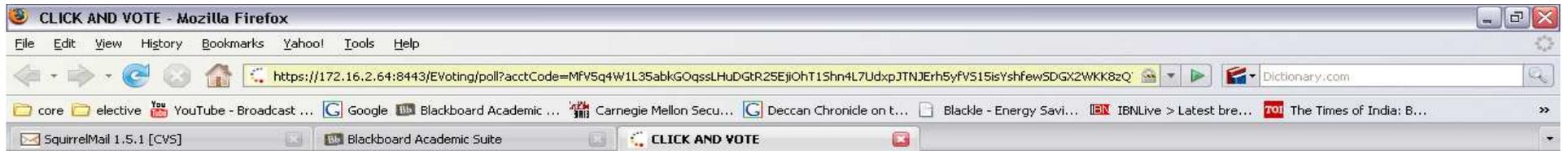
<https://172.16.2.64:8443/EVoting/poll?acctCode=MfV5g4W1L35abkGOgssLHuDGtr25EjiOhT1Shn4L7UdexpJTNJErh5yfVS15isYshfewSDGX?>

At the bottom of the interface, there is another set of navigation buttons: "Reply", "Reply All", "Forward", "As Attachment", "Delete", "Move to: INBOX", and "Move". A secondary navigation bar at the very bottom contains "[Previous | Next]", "[Delete & Prev | Delete & Next]", and "[Message List]". The status bar at the bottom left shows "Done" and the bottom right shows "webmail.andrew.cmu.edu".

Poll Invitee Interactions[4/11]



Poll Invitee Interactions[5/11]

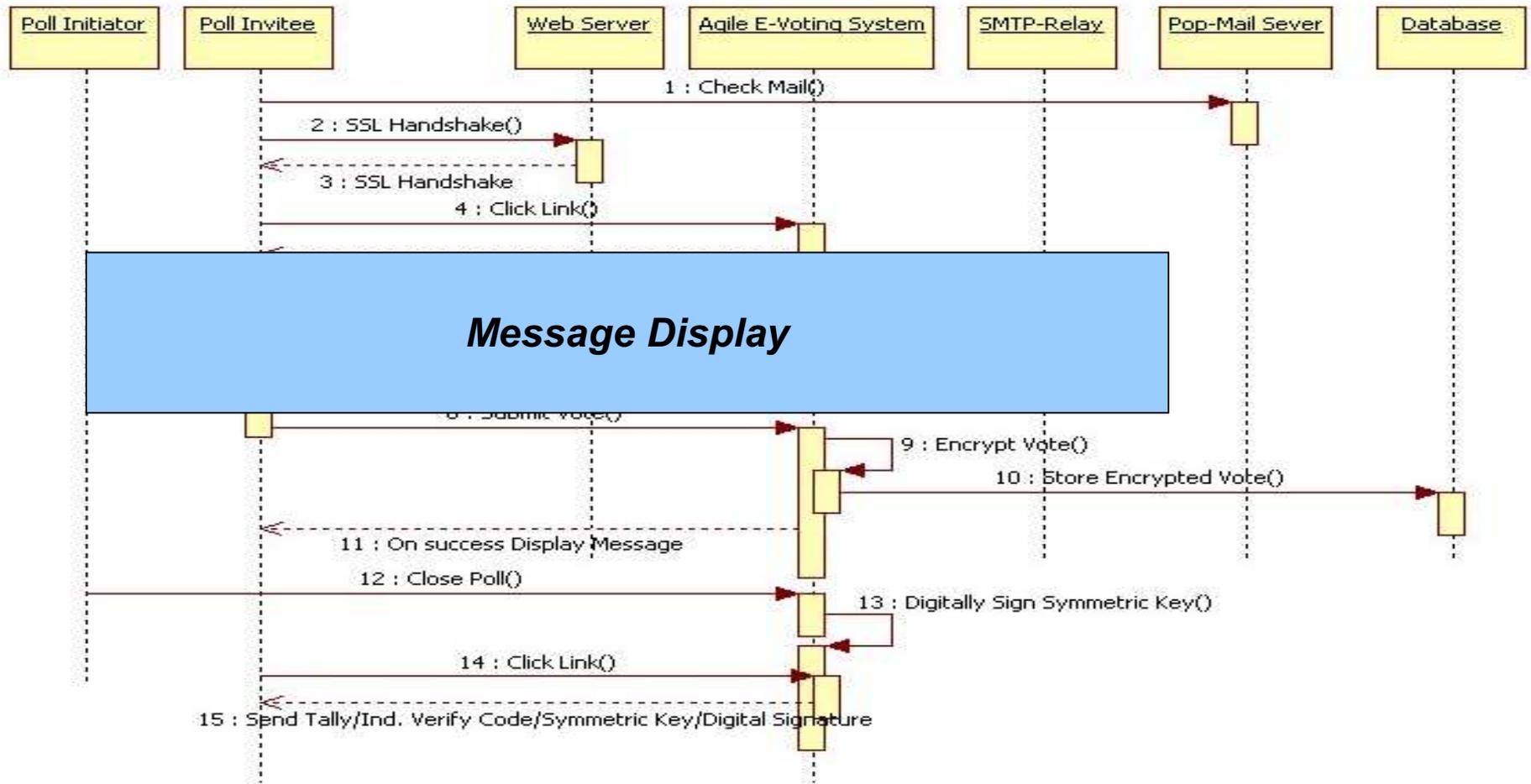


CMU CYLAB

POLL INVITEE ACCESS PAGE

Poll Name ASIANQatarTrip	
Poll Question	
Which of these two trips would you prefer?	
r?	
Candidates	
<input checked="" type="radio"/> Desert-Safari	
<input type="radio"/> Star-Cruise	
<input type="button" value="I-VOTE"/>	
Individual Verifiability Code	
<input type="radio"/> 3675	
<input checked="" type="radio"/> 7188	

Poll Invitee Interactions[6/11]



Poll Invitee Interactions[7/11]



CMU CYLAB

POLL INVITEE ACCESS PAGE

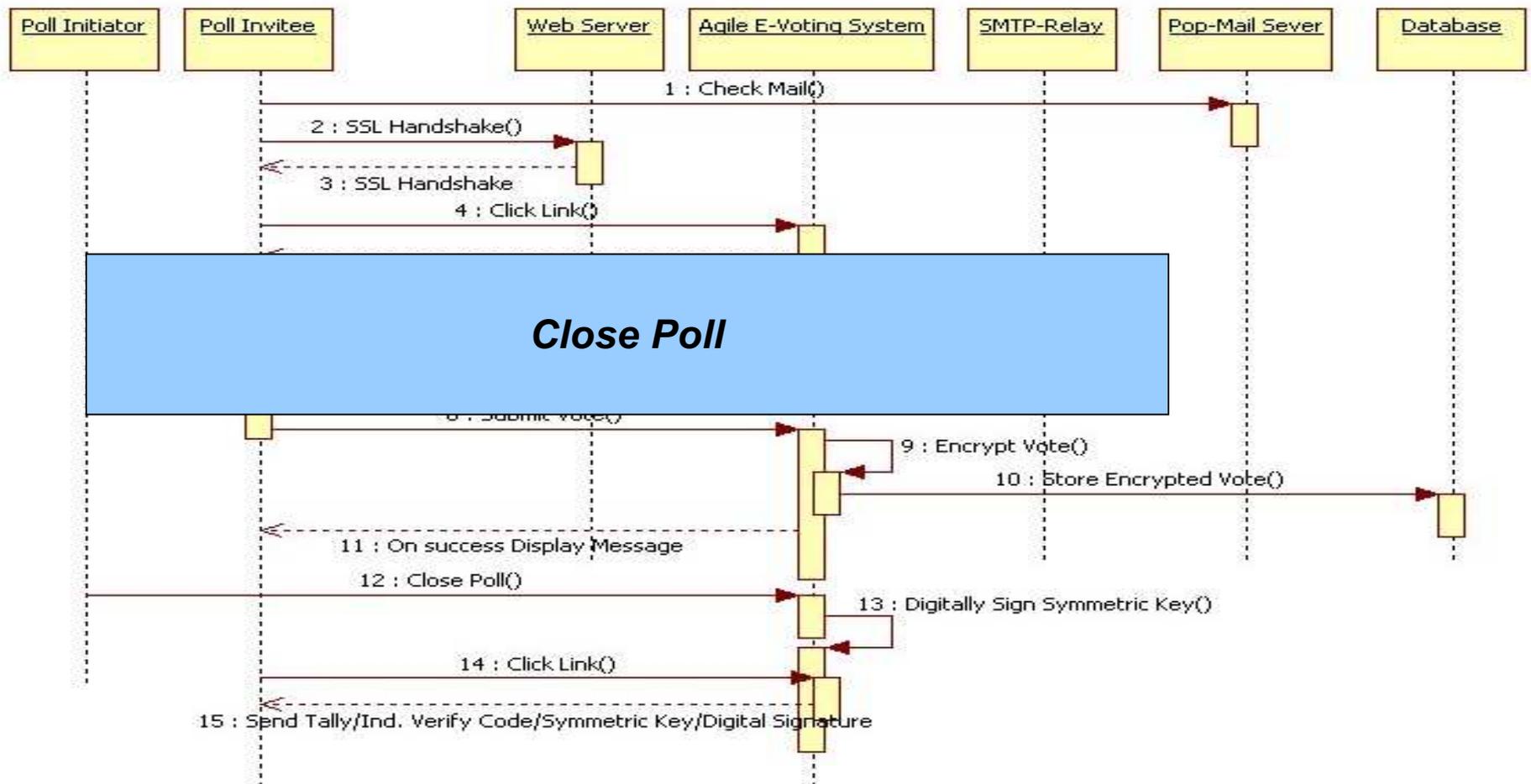
Thanks for Participating. Hail Democracy.

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.

Done

172.16.2.64:8443

Poll Invitee Interactions[8/11]



Poll Invitee Interactions[9/11]

The screenshot shows a Mozilla Firefox browser window with the following details:

- Browser Title: Please Store the Key for later use. - Mozilla Firefox
- Address Bar: <https://172.16.2.64:8443/EVoting/MyApplication.html>
- Page Title: CMU CYLAB
- Page Content: POLL INITIATOR ACCESS PAGE

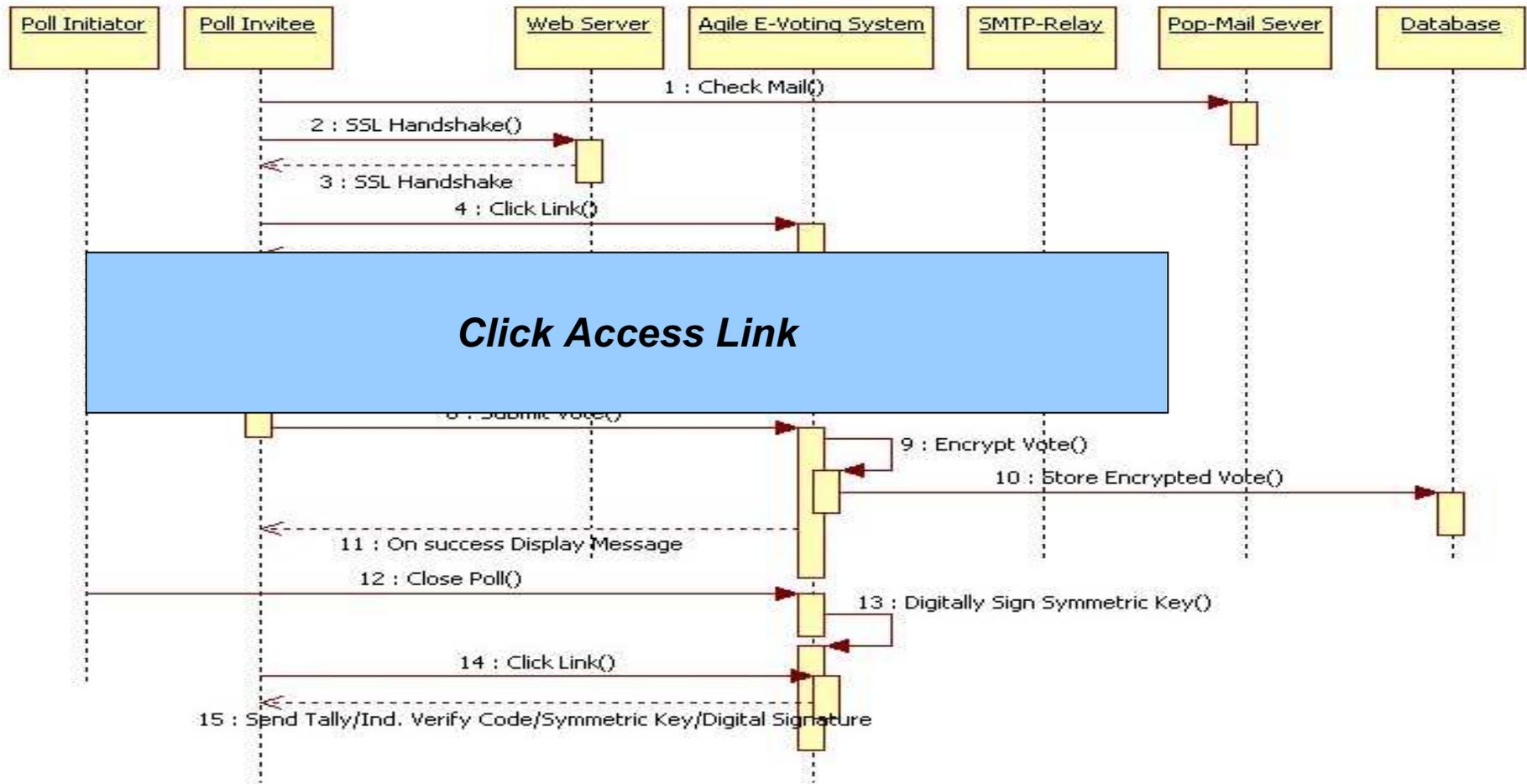
The main content area is a poll configuration form:

- Poll Name:** ASIANQatarTrip
- Poll Question:** Which of these two trips would you prefer?
- Multiple Selection:** false
- Poll Candidate List:**
 - Desert-Safari
 - Star-Cruise
- Message:** The above Poll is set to be closed. Please note that, once closed it cannot be re-activated again.
- Buttons:** Close Poll, Cancel

A left-hand sidebar menu is visible, containing the following items:

- User Account
 - CMUCYLAB
 - CMUJ
 - ASIANQatarTrip
 - Modify Poll
 - Send Ballot
 - Close Poll**
 - Delete Poll
 - IDOM
 - Nirvana
 - Place Poll
 - Presentation Turns
- MSITSeven

Poll Invitee Interactions[10/11]



Poll Invitee Interactions[1 1/1 1]

The screenshot shows a web browser window titled "CLICK AND VOTE - Mozilla Firefox". The page content includes a table of candidates, an "Encrypted Vote" section, a "Poll Invitee Hashed Access Code" table, and several cryptographic keys and signatures. Blue callout boxes with arrows point to specific fields and their cryptographic representations:

- $E_{K_{Poll}}\{\text{Vote}\}$ points to the "Encrypted Vote" field.
- $E_{K_{Poll}}\{\text{Ind. Verify Code}\}$ points to the "Individual Verification Code" field.
- $H_{SHA1}\{\text{Access Code}\}$ points to the "Poll Invitee Hashed Access Code" field.
- K_{Poll} points to the "Symmetric Key For this Poll" field.
- $S_{K_{Site}^{-1}}\{K_{Poll}\}$ points to the "Digital Signature of the Symmetric Key" field.
- K_{Site} points to the "Site's Public Key" field.

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

Encrypted Vote	Individual Verification Code
4ece745bd2220b5fa0f7d20ee81d8a89	f41fcdca538ec09fc851a805c535eb2e
1ae56ad6065744c4c7dbd779defa6f86	2b65388a0c365827f0bfb2377799

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

Symmetric Key For this Poll
f9c0ea55006ccd3c6842a143ad016071fc81dbb0f34ea18f

Digital Signature of the Symmetric Key
7d82ca0519eaf837c511e794e898fe6e3eb2d165a3af3dbfc8342e60044bcd674922496f7c5144fb401e422f6e9f8c1a8732c31e4711d667727d469749

Site's Public Key
30820122300d06092a864886f70d01010105000382010f003082010a0282010100e7cd82a31f056de7b1e54faa120524027c581f90b2b4efece67dc1cc24d905162e342ce2130e8

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 prefer?	
r?	
Candidates	
<input checked="" type="radio"/> Desert-Safari	
<input type="radio"/> Star-Cruise	
<input type="button" value="I-VOTE"/>	
Individual Verifiability Code	
<input type="radio"/> 3675	
<input checked="" type="radio"/> 7188	

Individual Verifiability[3/3]

CLICK AND VOTE - Mozilla Firefox

File Edit View History Bookmarks Yahoo! Tools Help

https://172.16.2.64:8443/EVoting/poll?acctCode=Mfv5q4W1L35abkGOqssLHuDGR25EjOhT1Shn4L7UdpxJTNJErh5yFV515isYshfewSDGX2WKK8zQ

core elective YouTube - Broadcast ... Google Blackboard Academic ... Carnegie Mellon Secu... Deccan Chronicle on t... Blackle - Energy Savi... IBNLive > Latest bre... TOI The Times of India: B...

SquirrelMail 1.5.1 [CVS] Blackboard Academic Suite CLICK AND VOTE CLICK AND VOTE

CIVIC LEAD

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
1ae56ad6065744c4c7dbd779defabf86	2b65388a0c365827f0bf2377793a5ca

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

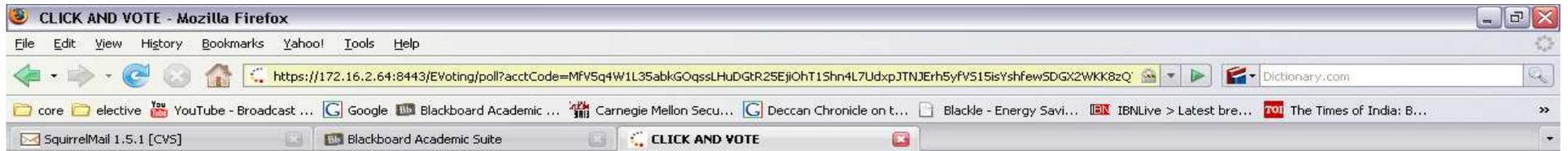
30820122300d06092a864886f70d01010105000382010f003082010a0282010100e7cd82a31f056de7b1e54faa120524027c581f90b2b4efece67dc1cc24d905162e342ce2130e8

Done 172.16.2.64:8443

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

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

Receipt- Freeness



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.

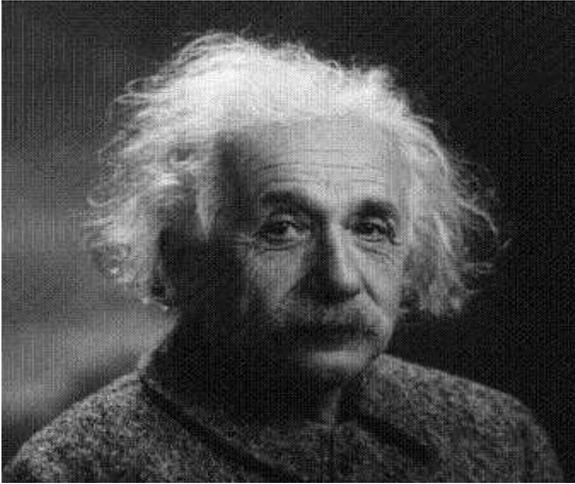
Done

172.16.2.64:8443

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