

mars/2004-12

# Anonymous Network (New)

Monday , 27th of December, 2004

Saburo Q. Kaneda ([kaneda@pst.fujitsu.com](mailto:kaneda@pst.fujitsu.com))

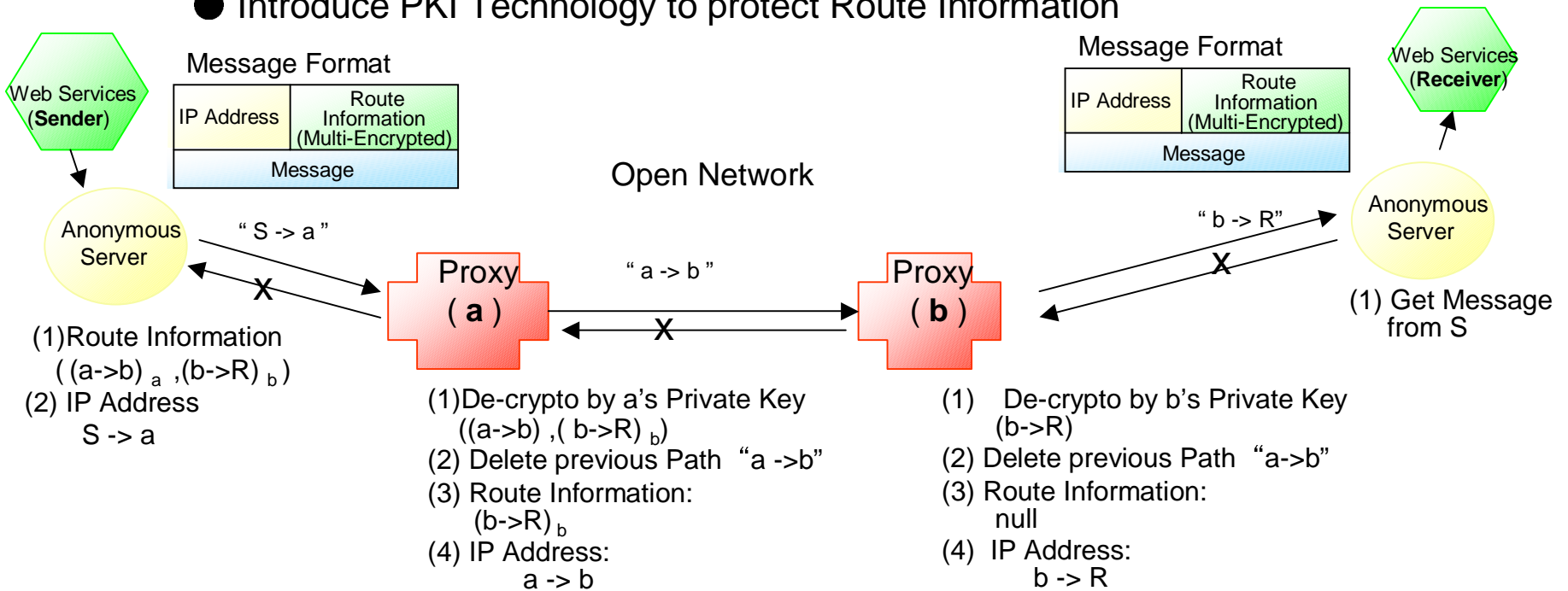
# RFP Summary

## 1. Objectives

- (1) As a Platform Independent Model of technology to protect Personal Information, including the Healthcare/Financial and others Application domain, “ Anonymous Network” Services are requested.  
The objectives are to protect Personal Information against Eavesdropping and Traffic Analysis with the following capabilities being essential:
  - (a) “Anonymous Network” Services to protect “ who” has posted the message to “whom”
  - (b) Mutual “Anonymity” Services to protect both of the Sender’s and Receiver’s anonymity
  - (c) Able to recover from failure of a segment of an anonymous Network route.
- (2) Platform Specific model (s) supporting a set of Anonymous Network Utility Interfaces for at least one open environment platforms( J2EE )

## 2. Current Onion Proxy Architecture

- Introduce “dedicated Plural Proxy Servers” on Open Network
- Send mail transmitting on plural Proxy Servers
- Proxy deletes Sender ID from Route Information
- Introduce PKI Technology to protect Route Information



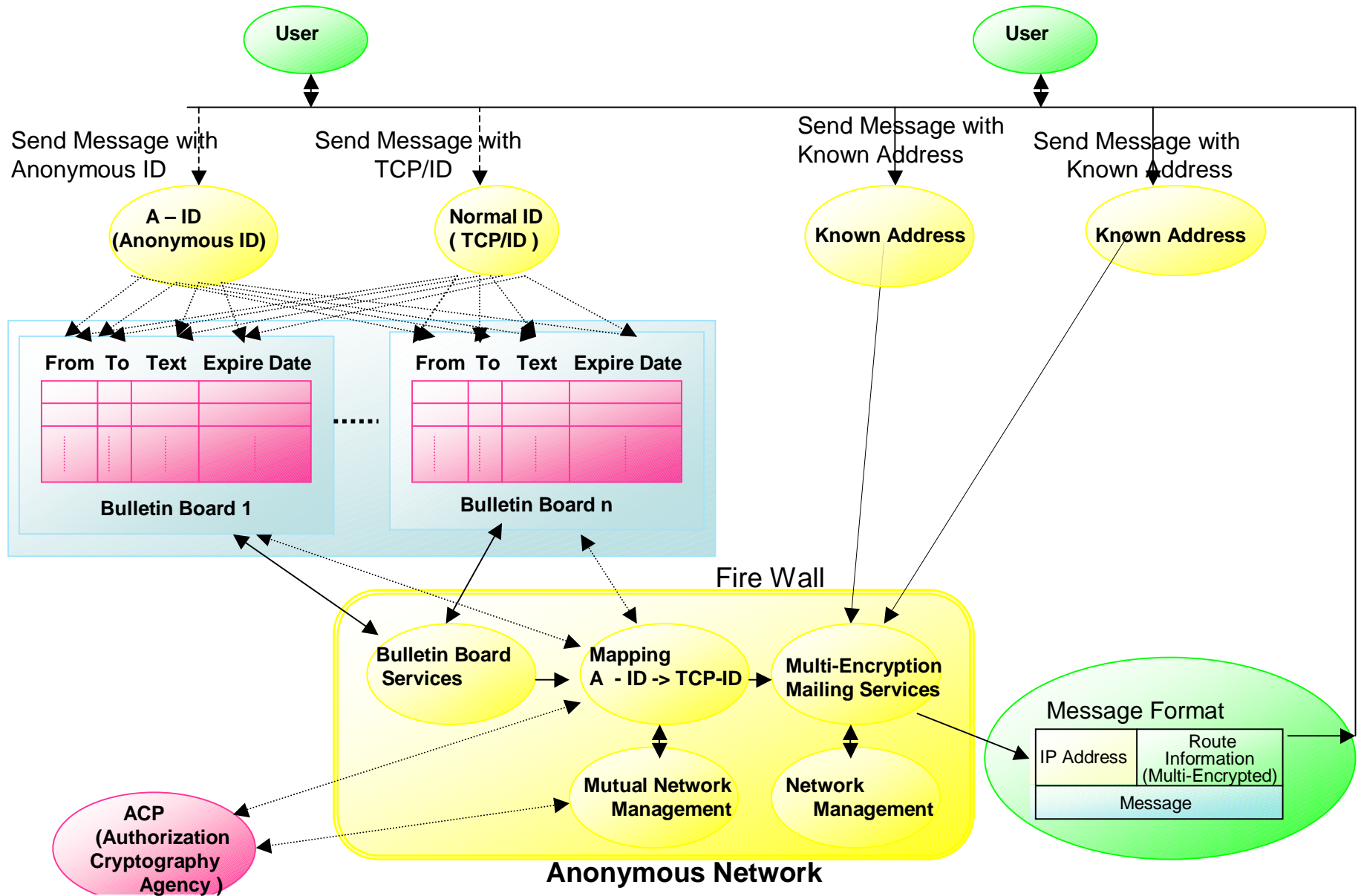
Legend:

- ((a->b)<sub>a</sub>, (b->R)<sub>b</sub>) : means
- There are path from Node a to b ,and R.
  - Route Information from Node a to Node b is encrypted by Node a's public Key.
  - Route Information from Node b to Node R is encrypted by Node b's public Key

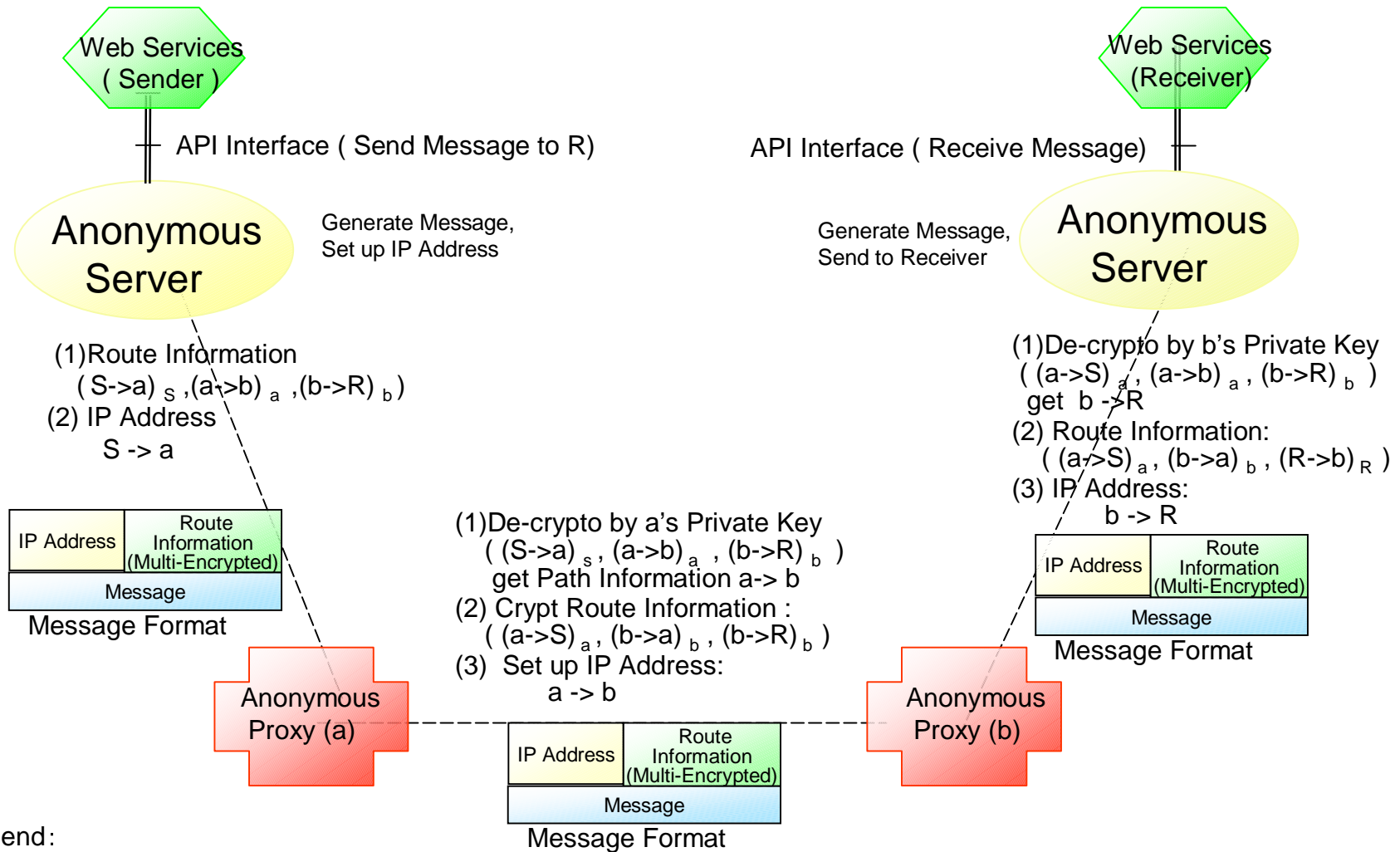
### Issues

- Route is fixed, so the path may be the Target of Attack
- Anonymity is not mutual

# 3. Anonymous Network Structure



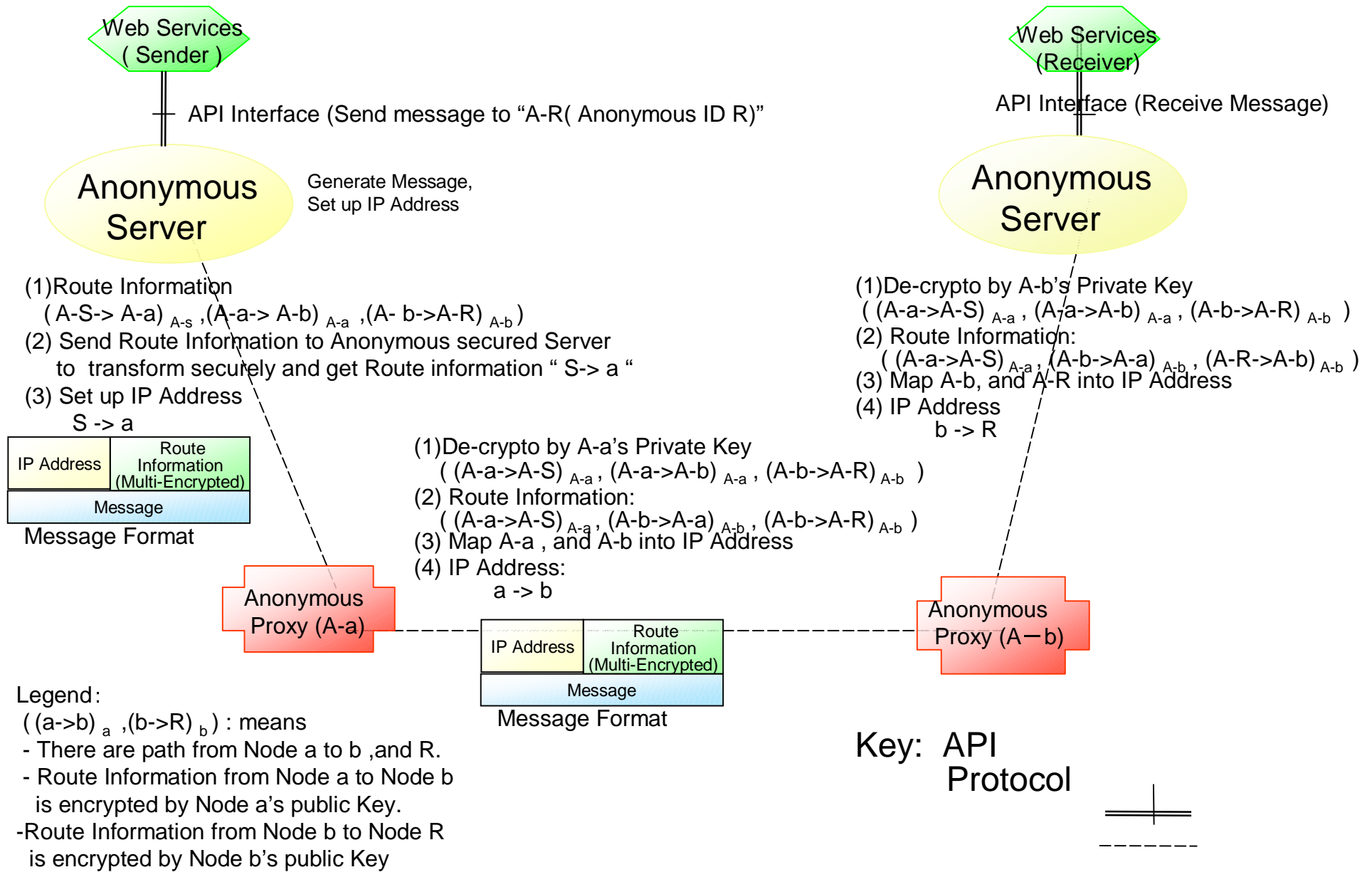
# 4. Anonymous Network between Nodes with Known Address



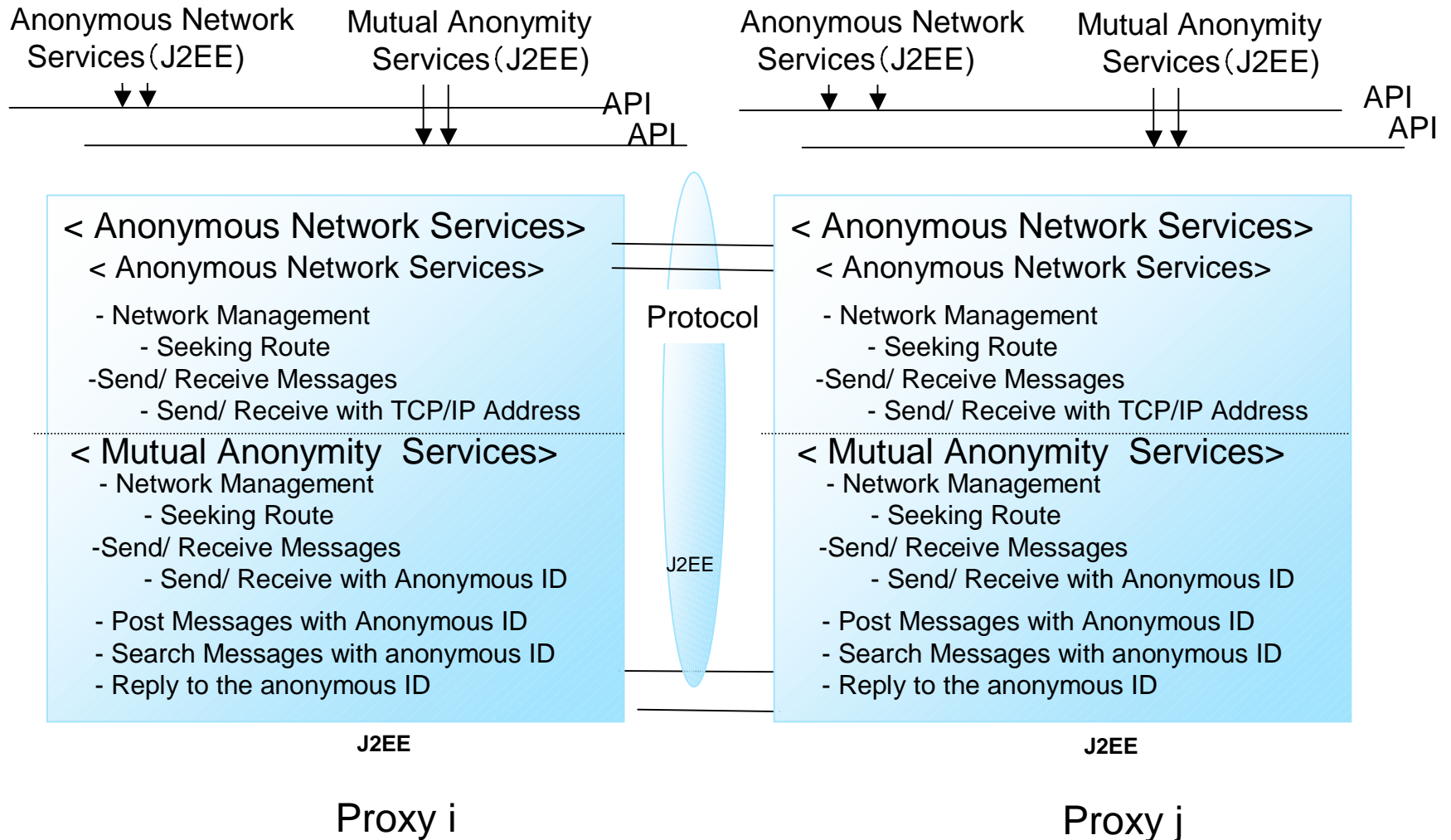
Legend:

- $((a \rightarrow b)_a, (b \rightarrow R)_b)$  : means
  - There are path from Node a to b ,and R.
  - Route Information from Node a to Node b is encrypted by Node a's public Key.
  - Route Information from Node b to Node R

# 5. Anonymous Network between with Anonymous ID



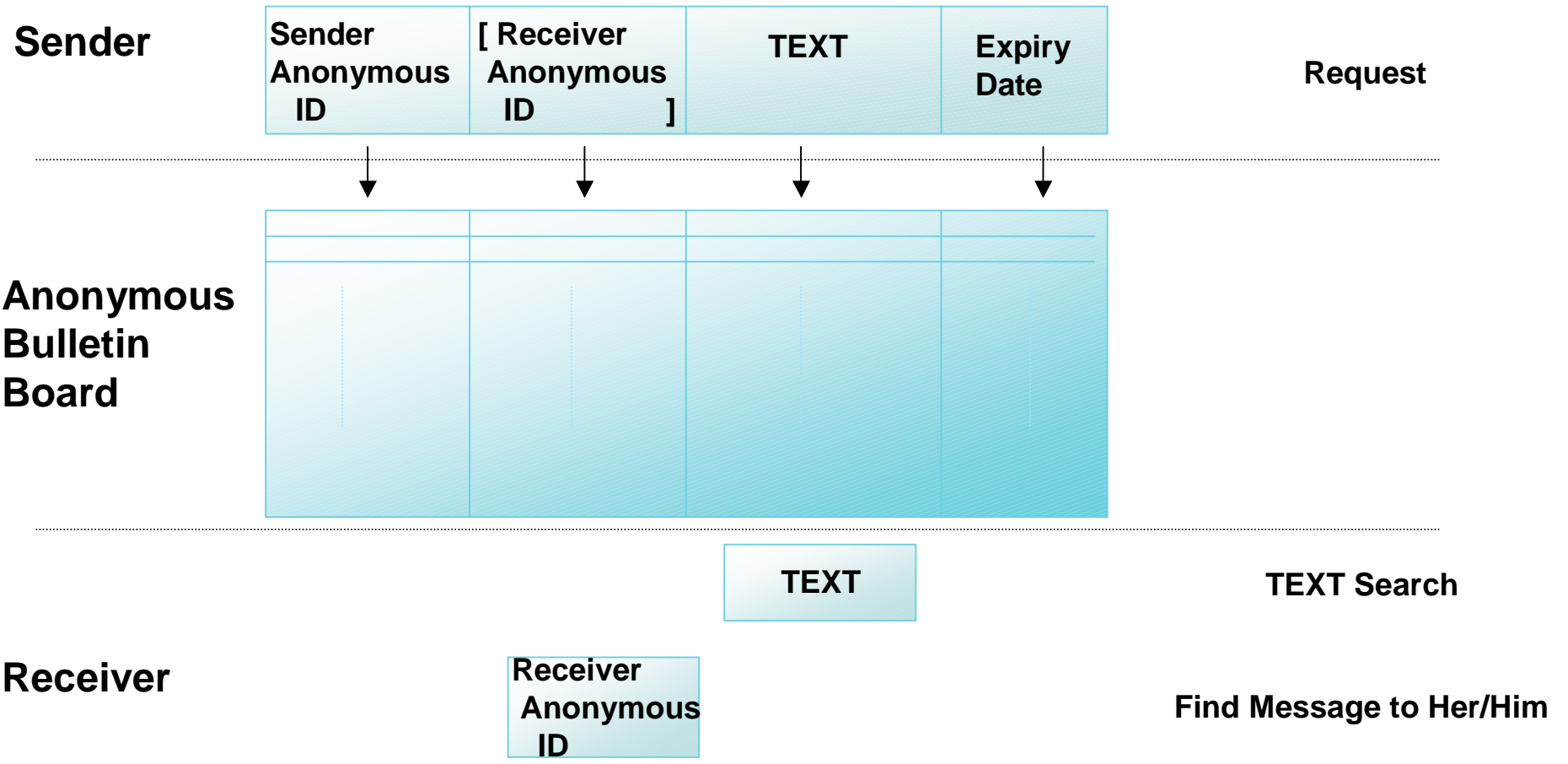
# 6. Services, API and Protocol



# Appendix

1. Mutual Anonymity
2. Anonymous Network APIs & Protocols
3. Anonymous Network Overview
4. Application

# <Appendix 1> Mutual Anonymity



\* Note  
Anonymous ID      Hashed Private Key      Random Number

# Anonymous Network Overview

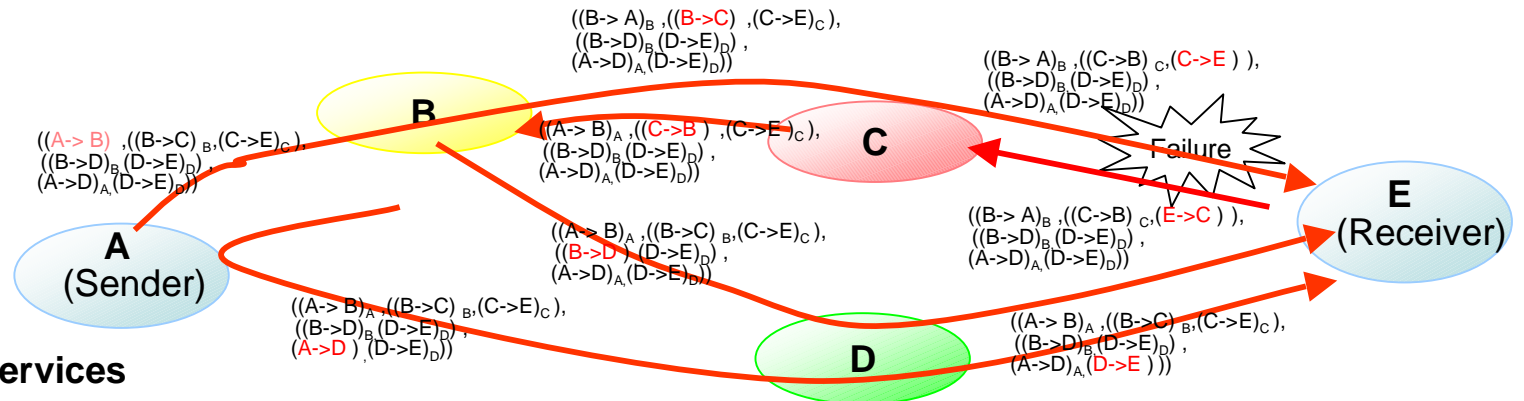
Healthcare, Finance, Home Defense, etc.

## Application Layer

Anonymous Network Services, Mutual Anonymity Services

### Anonymous Network Services

- < Network Management > At network establishment or Topology is changed, then define Network Configuration by Seeking Route
- < Forwarding/ Retrieving > Message Sending/Receiving



### Mutual Anonymity Services

- < Posting Messages with Anonymous ID >
- < Search Message Anonymously >
- < Reply to the anonymous owner of a searched Messages >

## Platform Specific Models

OMG IDL

CORBA

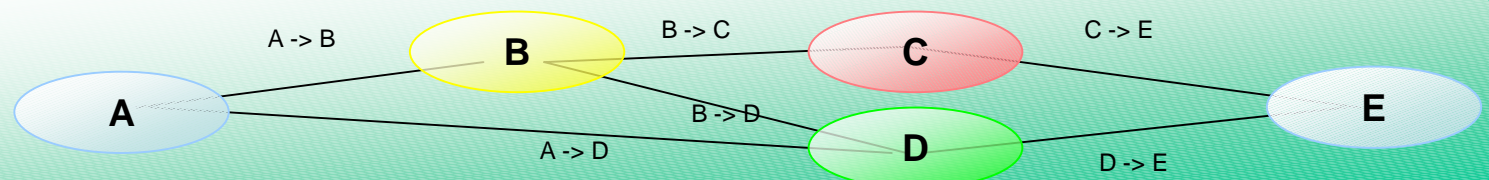
J2EE Interface

J2EE

Others

Others

## Internet Layer (TCP/IP)



# Applications

- (1) Healthcare Services to Protect Personal Information
- (2) Home Land Defense for Whistleblowers against Terrors
- (3) Financial for Whistleblowers to report anonymously wrongdoing without threat of retaliation .

# Anonymous Network RFP Mandatory Requirements (Mars :11-10-14)

- 6.5.1 Proposals shall provide a PIM for the Anonymous Networking capabilities requested below. The PIM shall incorporate both API interfaces for sender, receiver, and network management services AnonymousProxy exchange protocol operations and behavior.
- 6.5.2 Proposals shall provide PSMs of all the APIs and protocols expressed in the PIM, for one or more message exchange platforms, eg: CORBA, Java RMI, WSDL/SOAP, BEEP, and TCP/IP
- 6.5.3 Proposals shall Support the following anonymous Network Operations, specified in section 6.2. for an anonymous sender and a known receiver:SendAnonymousMessage, ReceiveAnonymousMessage
- 6.5.4 Proposals shall ensure that the Anonymous Network is able to recover from failed message sends.
- 6.5.5 Proposals shall include the following service, specified in section 6.2.1, to manage the establishment of Anonymous Network routes, EstablishRoutes
- 6.5.6 Proposals shall specify a Mutual Anonymity mechanism, supporting the following operations, specified in Section 6.2.2.:PostAnonymousMessage , PostReplyAnonymousMessage, SearchAnonymousMessages

# Anonymous Network RFP Optional Requirements (Mars :11-10-14)

- 6.6.1 Proposals may support the following Anonymous Network Services, specified in section 6.2.1 for an anonymous sender and an Anonymous receiver:
- SendAnonymousMessageToNodeWithAnonymousID, and
  - ReceiveAnonymousMessage