

# Lemonade Status Updates for IETF'65: Mar 22, 2006 WG session

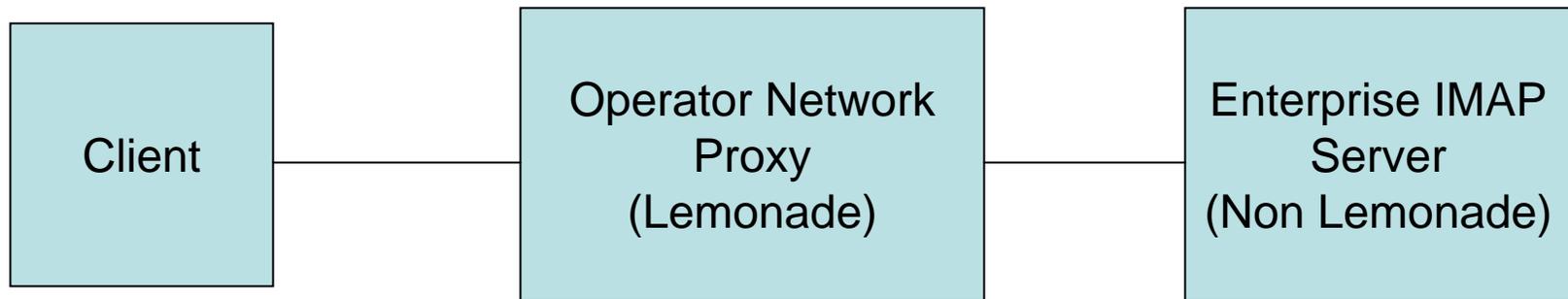
[stephane.maes@oracle.com](mailto:stephane.maes@oracle.com)

[ray.cromwell@oracle.com](mailto:ray.cromwell@oracle.com)

# draft-maes-lemonade-xencrypted-01

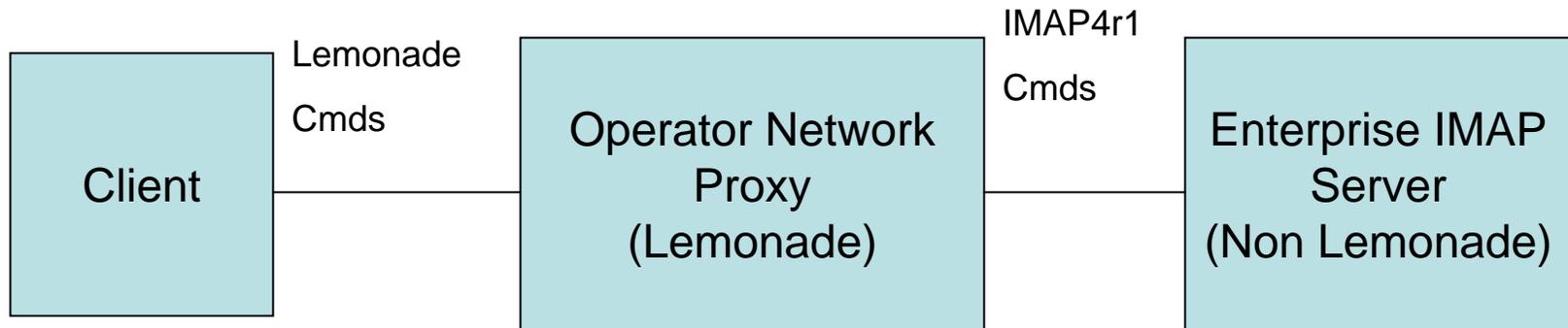
- Status update:
  - New draft for object encryption in answer to request for proposal
  - Address proxy based deployments identified by OMA
  - Discuss security issues / key management

# Operator Proxy Deployment Model



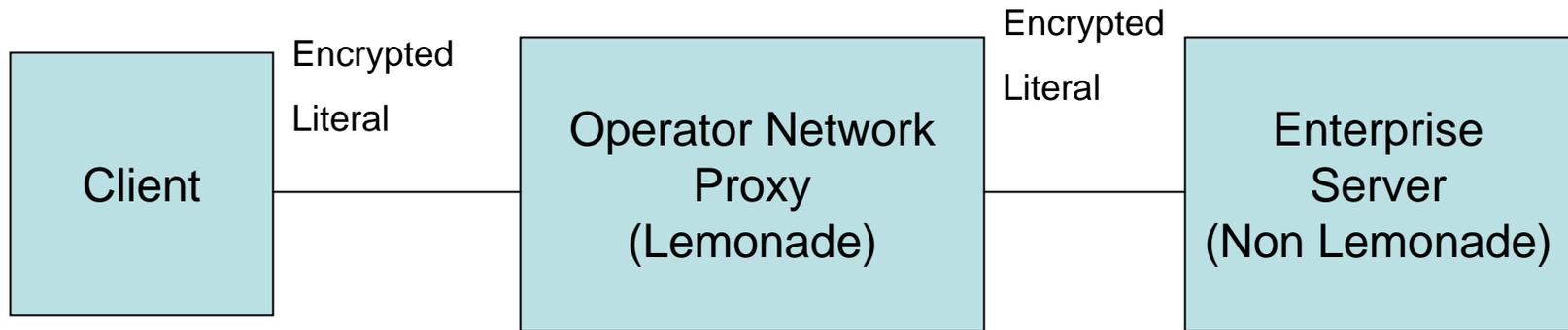
- Operator desires relationship with customer
- Operator wants to provide push-email like experience
- Operator wishes to provide this for enterprises which do not have Lemonade compliant servers deployed
- Enterprises demand security between the client and server

# Problem: Security



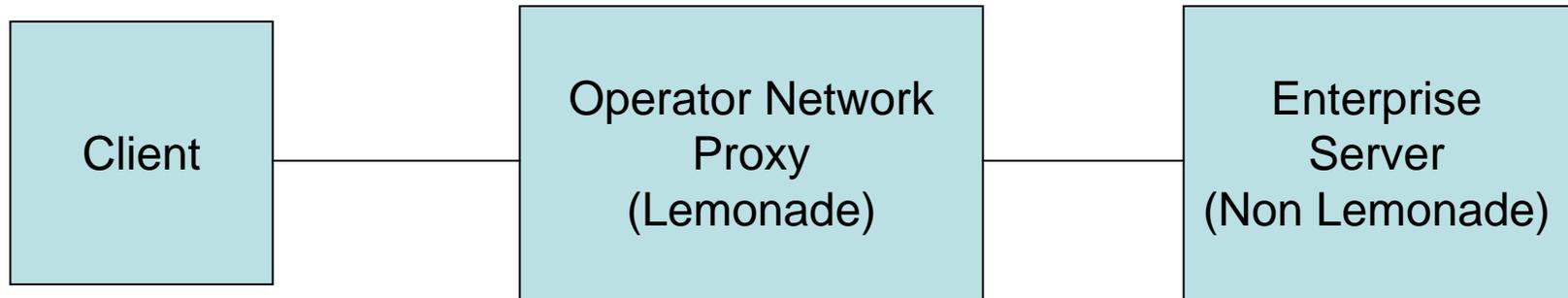
- Operator proxy cannot be pass-thru SSL/TLS tunnel because of the need to process Lemonade commands and responses
- Proxy must be able to issue IMAP commands on behalf of client to IMAP server
- Proxy must not be able to see non-protocol related information (message content)
- Proxy must not be able to spoof outgoing messages on behalf of user (fake message contents, replace distribution list or headers when sending email)

# Object Level Encryption



- Proposal: Object Level encryption. Introduce new “encrypted literal” syntax similar to IMAP binary
- Server decides which message attributes require confidentiality and integrity, and transmit data in encrypted literal format instead of as IMAP strings, literals, or literal8
- Proxy sees IMAP responses, but opaque message attributes, suitable for parsing and reformatting for Lemonade clients if necessary
- Client can create messages with Trio using encrypted literal

# Problem: Key Management



- Encryption keys must be securely negotiated between client and server
- Solutions?
  - Out-of-band transfer (another socket, SSL or HTTPS request, SMS or XDMS?)
  - Leverage SASL: SASL includes steps for client and server to compute a session key when confidentiality is requested
    - Introduce new type of SASL security request? Object-level vs transport level? Client and server perform all steps in SASL Digest of computing keys, but use them only for literals
  - Use custom key exchange IMAP protocol extension (yuck)

# Concerns covered in Draft

- Spoofing: Client APPENDs, proxy substitutes message
- Attacking with SMTP: Proxy uses URLAUTH+BURL to forward messages from IMAP to attacker address
- Proxy mutating flags (e.g. causing spurious deletions)
- Proxy substituting entirely fake messages in client view
- Many More!

# Challenging deployment model

- Clear that this model poses many risks
- Is not the preferred deployment model (preferred is Lemonade server or gateway at Enterprise)
  - It is demanded
- Right now, proprietary solutions exist that address these issues
  - A standard would be preferable
- Calling security experts to help
- Perfect solution to all of these concerns is not expected

# So, for draft-maes-lemonade-xencrypted-01 ...

- Next steps:
  - Rationalize integrity and confidentiality mechanism with SASL mechanism
  - More rigorous enumeration and definition of out-of-band key exchange mechanisms
  - Mechanism to prohibit proxy from obtaining URLAUTHs except as those specifically requested by client
  - Client Selective reveal of data for transcoding
  - Allow multiple encryption schemes? (CAPABILITY XENCRYPTED=3DES,RC4,AES etc)
  - Allow client to select preferred algorithm
  - Enhanced security concerns section, dealing with proxy hiding stronger encryption schemes
  - MUST implements (3DES?)
- Take to the list

# draft-ietf-lemonade-firewall-binding-00

- Status update: (Following Beijing's plan)
  - Carried over from draft-maes-lemonade-http-binding-04
  - Added REST and WebDAV binding discussion.
  - Clarified HTTP response codes.
- Editor's note:
  - Took name selected in Beijing BUT better name would be: mobile-network-binding or non-tcp-binding
  - ...
  - Motivation is not just firewalls but also and may be even more important the phone stacks and the network intermediary behaviors (e.g. TCP time-out on IDLE for 2.5G and even more for 3G)

# draft-ietf-lemonade-firewall-binding-00

- Next steps:
  - Should an OPTIONS HTTP request be supported to allow a client to probe HTTP binding capabilities, such as which protocol a given URL is bound to, or whether chunking is supported?
  - Should separate content types exist for IMAP and SMTP since the entity body in the HTTP request is different?
  - Standardizing the form of the URL for the binding may permit firewall administrations to impose better filtering.
  - Produce more rigorous rules for mapping IMAP and SMTP ABNF to SOAP, REST, and DAV.
  - Provide ways to declare supported bindings or select a binding.