Mapping of OMA Requirements to IETF Deliverables

1 Summary

This document is a response to the OMA MWG MEM liaison received by IETF LEMONADE specifically on the OME Mobile Email Requirements Document (Draft Version 1.0 – 14 Jun 2005).

It presents how Internet Email protocols and extensions being considered by the IETF LEMONADE WG along with OMA DM (device management) and IETF SIEVE, XCAP and SIP can meet these requirements.

2 Detailed Analysis

The requirements described in OMA-RD-MobileEmail-V1_0-20050614-D can be met fully through a combination of rich protocols designed for this intended use. The requirements can be broken into three categories :

1. Many requirements can be met with the base IMAP and SMTP-submit protocols, or with existing extensions.
2. Many requirments require new protocol development, most of which is within the scope of the IETF LEMONADE working group. Other protocol requirements may be met by related IETF working groups such as SIEVE.
3. Many requirements are implementation behavioral requirements on clients or servers that does not impact the underlying protocols. These may include requirements for auxillary protocols for support of configuration or accounting purposes.

Initial reaction:

· At a high level, the protocol requirements are addressed with the following technologies

- Mobile Client to server retrieval, message store management, foldering, server synchronization, and deletion is accomplished through IMAP V4 or extensions.
- Message submission is accomplished through SMTP-Submission in conjunction with extensions to IMAP for forward without download.
- Notifications are provided by a variety of network-specific technologies to include SMS and SIP Notify.
- Administration of the handset configuration can be accomplished through XCAP, SIP, or OMA Device Management protocols.
- Security including anthentication and encryption, and transport level compression are available in all IETF specified protocols listed above.

A more detailed review of the Mobile email requirements follows.

HLF-1	It MUST be possible to minimize delays and bandwidth requirements (e.g. by minimizing the number of roundtrips between client and server, the bytes to exchange between client and server, etc…) for the following:· ▪ Events sent from the server to the client or accessed by the client to announce or describe new e-mail

	▪ Exchanges to deliver new e-mail from the server to the client ▪ Events sent from the server to the client to announce or describe e-mail events on the server ▪ Events accessed by the client from the server to announce or describe e-mail events on the server ▪ Exchanges to reconcile the client after a e-mail event on the server ▪ Exchanges to access or manipulate attachments ▪ Sending e-mail from an assigned e-mail server ▪ Sending e-mail events on the client to the e-mail

The IMAP protocol is continually being optimized to deliver more functionality with fewer round-trips and with less computational and bandwidth overhead. Several LEMONADE extensions, including the quick-reconnect further reduce required bandwidth and message exchange. Other, more established extensions such as TLS compression will be profiled for use to minimize total number of bytes sent across the wireless link.

The specifics on the how IMAP and its various extensions currently support these requirements are described below in the rest of the requirement responses.

SEC-1	Events sent from the e-mail server to the client to announce or describe new e-mail MUST support confidentiality and integrity.

The challenge in this requirement is to ensure confidentiality and integrity across the internet, between an enterprise domain and a service provider's domain. Events may be announced via IMAP and via SIP, both of which support confidentiality and integrity. SMS also provides such support via services specific to SMS.

General comment on security requirements: IETF concept of 'end-to-end' is 'from sending user agent to receiving user agent'. Extrapolating from the context of the requirement SEC-1 through SEC-9, it appears that 'end-to-end', in these requirements, means 'from the handset client to their serving IMAP or SUBMIT server'. We have responded to these requirements assuming the latter definition. Note that virtually all IETF messaging and notification protocols are end-to-end secure in the IETF sense. That is, from sender to recipient. As a result, if we have mis-interpreted the meaning of SEC-1 through SEC-9, they can all be met with S/MIME or PGP. We would offer using terminology such as 'a secure connection from the client to the server' in future version of this document.

SEC-2	When used, events accessed by the client from the server to announce or describe new e-mail MUST be end-to-end confidential when desired.

Further clarification is requested on this requirement. End-to-end security is understood in the IETF as to require messages to be signed or encrypted at the sending endpoint and verified or decrypted at the receiving endpoint. Technologies to achieve this end are available through S/MIME or PGP, neither of which has seen broad deployment due to complexities in user experience and effective key management.

Note that the controlled environment of the mobile network makes key and certificate distribution considerably easier than in the general Internet. Thus we expect the widespread adoption of these technologies for mobile users.

With a more limited protection, hop-by-hop confidentiality can be provided. Both IMAP for retrieval and SMTP-Submit for message submission provide confidentiality between the client and server. Server-to-server confidentiality can be provided by using SMTP extensions for TLS.

SEC-3	Exchanges to provide new e-mail arrived on server to the client MUST be end to end confidential when desired.

IMAP, using TLS encryption provides confidentiality between the message server and the client.

SEC-4	When used, events sent from the server to the client to announce or describe e-mail events on the server MUST be end-to-end confidential when desired.

IMAP, using TLS encryption provides confidentiality between the message server and the client.

SEC-5	When used, events accessed by the client from the server to announce or describe w-mail events on the server MUST be end-to-end confidential when desired.

IMAP, using TLS encryption, provides confidentiality between the message server and the client.

SEC-6	Exchanges to reconcile the client after an e-mail event on the server MUST be end to end confidential when desired.

IMAP client synchronization events are confidential when using TLS encryption.

SEC-7	Exchanges to access or manipulate attachments MUST be end to end confidential when desired.

IMAP, using TLS encryption, provides confidentiality between the message server and the client.

SEC-8	Exchanges to send e-mail from the assigned e-mail server MUST be end to end confidential when desired.

SMTP-Submit, using TLS encryption, provides confidentiality between the message server and the client.

SEC-9	E-mail events sent from the client to the e-mail server MUST be end-to-end confidential when desired.

IMAP, using TLS encryption, provides confidentiality between the message server and the client.

SEC-10	The client MUST be able to be authenticated by the server when requesting data from the e-mail server.

IMAP using SASL authentication provides a variety of authentication mechanisms of varying cryptographic strength and can be integrated with a variety of network-based authentication server systems.

Alternatively IMAP user and password over a TLS session can provide authentication.

SEC-11	The server MUST be able to be authenticated by the client.

This is satisfied by using SASL with mechanisms that provide for mutual authentication (such as DIGEST-MD5).

SEC-12	Mobile email MUST support content screening.

What is content screening? Internet email has SIEVE as a filtering language that can be used to establish rules upon message deposit (including whether an attachment is of a particular type or size), and IMAP has searching and view capabilities to filter messages within the message store. Note that both of these mechanisms use filtering at the server so that only the result is sent to the client.

Sieve WG will be working on an extension to indicate what messages require server-to-client notification.

SEC-13	The mobile e-mail enabler MUST allow the mobile client to be protected by the same spam protection solutions as applied on the server.

Spam protection is primarily a server-side function. When using spam detection systems, the SPAM score can be utilized by IMAP searches and filters from the client as well as deposit-time SIEVE spamtest rules.

CHRG-1	In order to support charging for e-mail traffic, the mobile e-mail enabler SHOULD provide ways to identify mobile e-mail exchanges (events, access, sending, synchronization) as e-mail data exchanges, even when the exchanges are end-to-end secure.

Charging can be implemented in an IMAP and SMTP-Submit server using the diameter protocols without impact to the IMAP and SMTP protocol. All necessary charging information is provided within these protocols, even when delivered to the server in a secure fashion.

ADMIN-1	It MUST be possible to provision the mobile client from the server upon authentication and authorization of the user and pairing with a device.

This provisioning is outside the scope of the mobile email protocols by design, but can be provided by OMA Device Management, SIP or other OTA mechanisms used to provision other mobile applications.

ADMIN-2	It SHOULD be possible for user preferences/filters/settings to follow the user across devices, when desired by the user or administrator.

IMAP is a server-side mailbox that supports multiple simultaneous client access. Filters and settings are preserved without regard to the client that established them or access the mailbox

Sieve can be used to preserve filters between clients.

Terminal independent nature of internet email. Internet mail is device independent by design. Unless specficially composed for a given handset using a proprietary composition language, the common mail formats (text, HTML, RTF, PDF, etc.) render appropriately on multiple devices.

Need clarification on this requirement with respect to use of multiple… Simultaneous clients? Serial use of multiple clients.

Note that the IMAP protocol suite, including SIEVE, assume multiple simultaneous access of the mailbox by clients of differing capabilities. If this requirement is discussing the serial use of multiple clients, clearly the mechanisms that permit simultaneous access by diverse devices work for one-at-a-time access as well.

ADMIN-3	Authorized principals MUST be able to configure the settings of the user preferences/filters/configurable settings for a particular user.

The administration of the message store and submission server with default user preferences or to change existing preferences is outside the scope of the client-server MEM protocols. Such interfaces are possible and expected in message store implementations.

ADMIN-4	The mobile email enabler MUST support preventing or remotely revoking unauthorized usage of and access to e-mail data of a mobile device.

The mailbox server and submission server are the point of policy enforcement and the point where service can be denied.

These are centrally administered resources.

USAB-1	Mobile email SHOULD minimize event propagation delays and must not impose excessive delays according to user preferences.

IMAP and SMTP-Submit extensions under consideration in the LEMONADE working group of the IETF would further reduce event propagation delays, especially for problematic use-cases such as forwarding large attachments. Many latencies observed in existing mobile IMAP installations are the result of server implementation choices and not protocol issues. Requirements on implementations to optimize for wireless environments may be appropriate.

USAB-2	Mobile email SHOULD minimize delays in accessing email messages and must not impose excessive delays according to user preferences.

Currently, IMAP and Submit don't impose any excessive delays, and work is ongoing to further improve performance. IMAP, and IMAP with enhancements under consideration by LEMONADE provides a number of extensions to reduce delays. These include server side transcoding to reduce the size of a data element, Streaming download via a streaming server, and incremental partial download to begin rendering (listening/viewing) message content as it is downloaded.

It is also worth noting that an existing good practice by IMAP clients is to request an attachment in chunks and using command pipelining (overlapping the request for subsequent chunks to eliminate any round-trip latencies). This allows the client to abort the download at any point, and to resume it later at the point where it was left off.

USAB-3	When / if downloading an attachment, the client SHOULD be able to provide indication of the download and to estimate of the time needed to complete the download.

Clients can meter the data flowing to provide reliable estimates or use other measures of system throughput to predict the download time. This requires no explicit support in the transport protocol beyond the indication of content size. Such indication of content size is provided by IMAP.

USAB-4	E-mail sent from client MUST be sent to the e-mail server according to user preference if configurable or client settings otherwise, when network connectivity is available.

As a clarification, in the Internet Email model, email sent from the client is sent via the SUBMIT protocol to an outgoing mail submission server. Often the message store is separate from the submission server. For the case of forward-without-download, specific content may be retrieved from the message store by the submission server using standard protocols such as the URLAUTH and BURL extensions of IMAP.

The submission server may be configurable by the end-user or configured by an over-the-air provisioning protocol. When connectivity to the selected submission server is unavailable, outbound messages may be queued and retried at a later time.

USAB-5	When connectivity is not available or drops, if it is possible to compose and sent e-mail, it MUST be stored on the client until connectivity becomes available and then sent to the e-mail server as soon as possible.

IMAP and SMTP-Submit support off-line operations. IMAP changes will be synchronized with the message server when reconnected. Messages will be resubmitted via SMTP once connectivity is restored.

USAB-6	E-mail events on the client to the e-mail server MUST be sent to the e-mail server according to user preferences if configurable or client settings otherwise, when network connectivity is available.

This is a client implementation requirement.

USAB-7	When connectivity is not available or drops, email events on the client that may take place MUST be stored on the client until connectivity becomes available and then sent to the e-mail server as soon as possible.

This is a client implementation requirement.

USAB-8	The mobile email enabler MUST provide support for the user to be able to set filtering rules for the delivery of email based on: ▪ Email header fields ▪ Mailbox folder options. ▪ Server-determined spam score, Other criteria as needed.

SIEVE rules support all three criteria. Further IMAP searching capabilities can filter messages based on these criteria.

USAB-9	The mobile email enabler MUST provide support for the user to be able to change filtering rules from his mobile client.

The Manage Sieve protocol, LDAP, HTTP, or XCAP can be used to configure SIEVE rules. Selection of one for the MEM enabler is expected.

USAB-10	Rules (like filtering rules, processing rules, attachment removal, spam prevention, …) applied on the server MUST still apply to the repository on the client for what the user has selected to synchronize on the client.

IMAP client can synchronize with the server, so any rules-based filtering, flag-setting, or header modifications are replicated to the client.

USAB-11	The mobile email enabler MUST provide support for the user to be able to select the default or available ways to be notified about new e-mails based on capabilities of client and network: ▪ what notification is used (e.g. SMS, Push, MMS, …) ▪ if events are accessed by client (when, how, what is initially part of the event)

This needs to be discussed in the context of the OMA activities. SMS, WAP-Push, and MMS are out-of-scope for IETF activity; however, extensions to SIEVE to indicate specific notification technology may make sense.

USAB-12	The mobile e-mail enabler MUST support the use of a number of different means to transport notifications (e.g. SMS, MMS, WAP Push, SIP Notification, UDP, in band, polled, …). This will allow. deployment on any target networks.

The filtered notification of new messages must be profiled on a network technology basis.

Notifications, other than IMAP synchronization update or SIP NOTIFY, are essentially out of scope for the IETF. Note that work is underway for a bulk server-to-server notification protocol, which would enable non-EITF notification servers (such as SMS, MMS and WAP push).

USAB-13	The User MUST be able to select how e-mail server should present new e-mail events to the client and to select how the client reacts to such events and therefore how the new e-mail is reflected in the client repository: ▪ A few meta-data, no stored e-mail ▪ A given size of the e-mail ▪ The whole e-mail without attachment ▪ The whole e-mail with attachment

IMAP supports each of these modes of operation under the control of the client. The client implementer can consider user input into the choice of how the client reacts as appropriate. IMAP also supports additional modes not listed that may be useful for mobile clients, such as fetching a specific attachment or chunking the response.

USAB-14	The user MUST be able to manually initiate access to e-mail that has arrived on the server but is not yet on the client.

IMAP supports retrieval of messages in the absence of prior notification. IMAP can be used in this polling methodology or used as an external notification-triggered poll.

USAB-15	The user MUST be able to manually access more e-mail data when only a portion is stored on the client (e.g. more of the body, a specific attachment, more of a specific attachment, the rest of the body, the whole e-mail with all attachments).

The IMAP protocol supports local replication of a subset of mailbox data, under the control of the client as a part of the base IMAP spec.

USAB-16	Authorized principals MUST be able to select the default or available ways that -mail events are sent to or accessed by the client and other e-mail settings that may affect the server behaviour.

This is a requirement for an authorized principle to change the configured behaviours of the IMAP client. Such configuration can be specified in an OMA profile and managed with an OTA provisioning protocol or through an extension to the IMAP protocol itself. Further, authorized principles may manage SIEVE rules on the server, independent of the client, to affect server behaviour.

USAB-17	The mobile e-mail enabler SHOULD NOT require repetitive actions by the user to provide robustness to intermittent or unreliable connectivity (e.g. loss of connectivity, loss of network transport packets and reconnect) (e.g. having to initiate client reconnect, initiation of synchronization, password entry for server authentication, VPN re-establishment, etc…).

This is a client implementation and handset OS issue. The Internet mail protocols support transparent retries, retransmissions, and graceful failure.

USAB-18	The mobile email enabler MUST enable the user to forward an e-mail with attachment without downloading the attachment to the client.

This is supported in the LEMONADE phase-1 profile, which indicates the coordinated use of two IMAP and one SMTP-submit extension (a.k.a, ‘the trio’)

USAB-19	The mobile email enabler MUST enable the user to forward an e-mail partially downloaded without having to download the remainder to the client.

This is supported in the LEMONADE phase-1 profile, which indicates the coordinated use of two IMAP and one SMTP-submit extension (a.k.a., ‘the trio’)

USAB-20	The mobile e-mail enabler SHOULD minimize the amount of information that a user must provide to provision an e-mail client to access the appropriate e-mail server.

The amount of information a user must provision is a factor of the integration with over-the-air provisioning. In the absence of such provisioning, the user may be required to enter username, password, SMTP-submit server and IMAP server names. Alternately, integration with mobile network identity services may utilize existing handset identity facilities to reduce this to zero user-provided information.

USAB-21	The client MUST allow the user to reply to an e-mail partially downloaded without first having to download the remainder of the e-mail to the client.

The client may construct a reply after downloading only the message headers. Replies that include selected body parts may do so without downloading those parts through the forward-without-download extensions (i.e., the trio described before). Through use of the CATENATE extension, the client can compose a message using a template that may include new or modified content from the client and unmodified content residing on the server. For example, a reply message may include a modified text introduction and a picture excerpted from another message in a reply, without downloading the picture.

USAB-22	The client MUST allow the user to edit a partially downloaded e-mail, for reply and have the resulting e-mail sent from the server.

The client may construct a forwarded message with or without downloading any of the original message. Forwarded messages that include only selected body parts may do so without previously downloading those parts through the forward-without-download extensions. Further options are possible such as forwarding several messages together in a single enclosing message.

USAB-23	The client MUST allow the user to edit a partially downloaded e-mail , for forward and have the resulting e-mail sent from the server.

See response to USAB-22

USAB-24	The client MUST be able to download body parts or parts thereof that the user wants to edit when replying to an e-mail partially downloaded to the client.

See response to USAB-21

USAB-25	The client MUST be able to download body parts or parts thereof that the user wants to edit when forwarding an e-mail partially downloaded to the client.

See USAB 21

USAB-26	When replying to a long list of addressees, the client MUST allow the user to edit the addresses.

This is a client implementation requirement.

USAB-27	Mobile-email Enabler SHOULD support multiple email accounts.

This is a client implementation requirement. Most IMAP clients already support this.

USAB-28	Mobile-email Enabler MUST support configuration of email account information for connection and filtering on a per-account basis.

This is a client implementation requirement. Most IMAP clients already support this.

USAB-29	Mobile-email Enabler SHOULD support definition of auto-reply messages for filtered messages. Automatically generated replies MUST conform to RFC 2821 and related RFCs and MUST NOT lead to mail loops.

Further clarification on this requirement is solicited. There are several points where filtering can be applied, both before and after the SIEVE rules where auto-reply rules normally operate. SIEVE rules to control auto-reply messages are currently defined.

USAB-30	Mobile-email Enabler SHOULD support activation/deactivation of auto-reply from the client. Automatically generated replies MUST conform to RFC 2821 and related RFCs and MUST NOT lead to mail loops.

Manage sieve protocol, LDAP, HTTP, XCAP or other protocol can be used to set or update the auto-reply message rules and the auto-reply message(s) themselves.

USAB-31	Mobile-email Enabler MUST support replying to messages by using the email account that the original message was received on.

This is a client implementation requirement.

USAB-32	Mobile-email Enabler SHOULD support organization of the retrieved email messages according to their source email account.

This is a client implementation requirement

USAB-33	The mobile enabler MUST support the user ability to forward only a selection of the attachments of an e-mail with attachments, without downloading the attachments to the client.

See response to USAB-22

USAB-34	The mobile e-mail enabler MUST provide mechanisms to access any desirable email part even when the email size is beyond the limit imposed on the size of the emails that can be delivered to mobile devices while remaining within the size constraints of the part to be downloaded

IMAP can support downloading a single attachment of a set. IMAP also permits fetching just a portion of a single attachment. Depending on the content-type of the attachment, this capability allows a streaming rendering of the large content via a sequence of partial fetch operations. LEMONADE phase-2 is expected to specify the use of external streaming servers with optional transcoding to further improve the user experience.

IOP-1	Data exchanges between the client and server, such as Events, sending Mail, reconciliation, attachment manipulation MUST remain functional in the presence of firewalls between the mobile e-mail client and the users e-mail servers.

Internet email protocols are used through firewalls and have demonstrated security through standard deployment topologies. Use of standard protocols leverages the investment in firewall security software designed to perform protocol and content inspection per corporate policy.

IOP-2	When used, events sent from the server to the client to announce or describe new e-mail MUST be network neutral.

Client to server notifications are supported in both IMAP and SMTP, both over TCP/IP data networking. The data networking is a common convergence layer from many sub-network technologies. TCP/IP provides robust transport services across many sub-network performance characteristics.

IOP-3	When used, events accessed by the client from the server to announce or describe new e-mail MUST be network neutral.

Client to server notifications are supported in both IMAP and SMTP, both over TCP/IP data networking. The data networking is a common convergence layer from many sub-network technologies. TCP/IP provides robust transport services across many sub-network performance characteristics.

IOP-4	Exchanges to provide e-mail arrived on server to the client MUST be network neutral.

Notifications can be delivered to the client through any “always on” channel available to the client. The choice of channel does not impact the nature of the subsequent retrieval using IMAP over TCP/IP.

IOP-5	Exchanges to reconcile the client after a e-mail event on the server MUST be network neutral.

Client to server notifications are supported in both IMAP and SMTP-submit, both over TCP/IP data networking. The data networking is a common convergence layer from many sub-network technologies. TCP/IP provides robust transport services across many sub-network performance characteristics.

IOP-6	Exchanges to access or manipulate attachments MUST be network neutral.

Client to server notifications are supported in both IMAP and SMTP, both over TCP/IP data networking. The data networking is a common convergence layer from many sub-network technologies. TCP/IP provides robust transport services across many sub-network performance characteristics.

IOP-7	It MUST be possible to send e-mail from the e-mail server assigned to the user (e.g. not another SMTP server in another domain).

Best current operational practices require that mail be sent through the user's assigned mail server and not through unauthenticated open or third-party relays. These best practices are supported by the SMTP-Submit protocol.

IOP-8	Sending e-mail from an assigned e-mail server MUST be network neutral.

Client to server notifications are supported in both IMAP and SMTP, both over TCP/IP data networking. The data networking is a common convergence layer from many sub-network technologies. TCP/IP provides robust transport services across many sub-network performance characteristics.

IOP-9	Sending e-mail events on the client to the e-mail server MUST be network neutral.

Client to server notifications are supported in both IMAP and SMTP-submit, both over TCP/IP data networking. The data networking is a common convergence layer from many sub-network technologies. TCP/IP provides robust transport services across many sub-network performance characteristics.

IOP-10	The mobile e-mail enabler MUST allow the e-mail repository on the mobile client to be synchronized with the appropriate backend server: ▪ Sometimes via the OMA Mobile e-mail enabler specifications (between client and server) ▪ Sometimes via the OMA DS specifications for e-mail between the client and another client, that it be o Connected to the server o Previously synchronized with the server and later re-synchronized with the server

IMAP supports the synchronization of email between multiple terminal devices and server. Use of DS is outside the scope of Internet email protocols.

IOP-11	The e-mail enabler MUST support server-side adaptation of attachment to the device user by user.

Server-side transcoding and the necessary security infrastructure is a work item for LEMONADE phase 2.

IOP-12	The server-side adaptation MUST be capable of being controlled by the client (e.g., with smart or intermediate clients).

Server-side transcoding will be under the control of the client is a work item for LEMONADE phase 2.

IOP-13	The design of the mobile e-mail enabler specifications SHOULD consider and aim at interoperability or gracefully degradation with relevant e-mail standards.

Internet email protocols are designed for backward compatibility and degrade gracefully when interoperating with less capable elements. Transcoding capabilities will augment this flexibility by bring this flexibility to the content plane.

IOP-14	The number of optional features in the Mobile E-mail enabler specifications SHOULD be minimised, while allowing efficient implementation of both consumer and enterprise mobile e-mail solutions.

The intent of the LEMONADE profile is to define a base specification of must implement features for servers. Clients may use these capabilities as required to deliver the desired user functionality. Similar philosophy can be applied to elements of the mobile email enablers not covered by LEMONADE.

IOP-15	Server-side adaptation MUST preserve the ability of accessing e-mail via other channels (e.g. via other e-mail clients).

IMAP supports simultaneous access to messages by multiple clients. Anticipated server-side transcoding solutions will leave the original content intact for rendering by less restricted clients or in less restricted connectivity environments.

IOP-16	Server-side adaptation MUST preserve the original e-mails and attachment stored in the e-mail server

LEMONADE anticipates retaining the original attachments and email for rendering or forwarding by more capable, or better connected clients when available.

PRIV-1	The mobile e-mail enabler MUST allow the mobile client to be protected by the same privacy protection rules / solutions as applied on the server (e.g. filtering rules, privacy alert detections on outgoing e-mail, read/unread notice interception).

This is a client implementation requirement. IMAP makes available the standard flags, rules, and filters available to the server. Further, IMAP provides explicit support for read/unread notices across multiple clients.

PRIV-2	The mobile e-mail enabler MUST support the use of privacy tools that

	require user's confirmation before allowing some e-mail events to take place.

This is a client implementation opportunity to gather user confirmation when appropriate to enhance the users privacy. The IMAP and SMTP-Submit protocol offer no obstacle to a rich confirmation environment.

SYSREQ-1	The mobile e-mail enabler MUST be robust enough to operate normally and useably when there is a intermittent or unreliable connection between the client and server.

LEMONADE phase-1 provides quick reconnect functionality to reduce the overhead of the often frequent reconnections necessary to deliver the user experience. Further, there is work within IETF and other bodies to address the quality of TCP/IP implementation in underlying mobile networks. As this work advances, the usability will further increase without additional changes in the application protocols.

SYSREQ-2	The mobile e-mail enabler security (authentication, authorization, confidentiality, integrity) MUST operate and be usable in the presence of intermittent or unreliable connectivity (loss of connectivity, loss of network transport packets and reconnect).

The quick reconnect extensions to IMAP were designed for this use case.

SYSREQ-3	The mobile e-mail enabler MUST NOT rely on the storage of email data in intermediate systems outside the e-mail server domain or the terminal.

When the IMAP and SMTP-Submit servers are deployed inside the email server domain, there is no copy of the email stored outside that domain except that which is retained in the terminal. Both IMAP and SMTP-submit were designed with this requirement in mind.

SYSREQ-4	Mobile e-mail enabler MUST permit highly scalable end-to-end implementations.

Internet email protocols are used in the worlds largest email installations and scale horizontally and vertically.

SYSREQ-5	The mobile e-mail enabler SHOULD allow optimized implementations on constrained devices (e.g. power consumption, CPU overhead, memory and storage requirements). See also OMA-RPT-ApplicationPerformance-v1-20031028-A for additional informative details.

The primary intent of LEMONADE is to define protocols suitable for use in constrained devices or in constrained connectivity situations.

MEC-1		Mobile email client MUST be able to authenticate the mobile email server when a request is received from that server.

The push of the events outside the IMAP session are authenticated per the domain in which they are designated. The retrieval of message content initiated by the notification is always authenticated. When an IMAP connection is active, push events are delivered within the IMAP session using the same authenticated session.

MEC-2		It MUST be possible to protect E-mail data on the mobile e-mail enabler client from unauthorized access.

This is a client implementation issue.

Various implementation techniques can be used to protect the client from unauthorized access.

MES-1		Mobile email server MUST be able to authenticate the mobile email client when a request is received from the client.

The IMAP and SMTP-Submit protocols require authentication prior to initiating any events.

NIF-1	P2P/Corp, Client email events	Interfaces between mobile email client and mobile email server MUST support secure transportation of data and event notification.

Both IMAP and SMTP-Submit support the invokation of TLS security for secure transportation of data and event notification. Securing the notifications delivered out-of-band through protocols such as SMS are secured by techniques optimized for their domain.

3 Recommendation

This document contains a response to the OMA MWG MEM liaison by IETF LEMONADE specifically on the OME Mobile Email Requirements Document.

We recommend:

- Any new protocol work required to enhance Internet Email be undertaken in the IETF LEMONADE and other relevant IETF messaging related WG’s
- The OMA MEM enabler reference the LEMONADE profile for protocol related requirements. The LEMONADE WG will continue close liaison to ensure the LEMONADE profile meets the approved requirements of the MEM enaber.
- The OMA MEM SWG focus on the architecture and specification of implementation and behavioural aspects of the mobile email requirements.
- Individuals with an understanding of the OMA Mobile Email RD are strongly encouraged to participate in the LEMONADE work in IETF

IETF LEMONADE looks forward to working with OMA MWG MEM to fulfill your requirements.