

# 通 信 标 准 类 技 术 报 告

YDB 028—2009

---

## 移动电子邮件业务技术要求

Technical requirements for mobile Email Service

2009-04-29 发布

---

中国通信标准化协会 发布

# 目 次

前言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语、定义和缩略语 .....	1
3.1 术语和定义 .....	1
3.2 缩略语 .....	4
4 业务描述 .....	4
5 功能要求 .....	5
5.1 接收邮件 .....	5
5.2 接收电子邮件通知 .....	6
5.3 接收大邮件 .....	6
5.4 阅读邮件附件 .....	6
5.5 发送邮件 .....	7
5.6 改变过滤规则 .....	7
5.7 客户端之间的数据同步 .....	7
5.8 带有附件的邮件 .....	7
5.9 在下载附件的情况下转发邮件 .....	7
5.10 配置电子邮件帐号 .....	8
5.11 回复邮件 .....	8
6 网络结构 .....	8
6.1 架构 .....	8
6.1.1 组件 .....	9
6.1.2 接口 .....	10
6.1.3 移动电子邮件客户端 .....	13
6.1.4 移动电子邮件服务器 .....	15
6.2 流 .....	17
6.2.1 在使用移动电子邮件服务之前 .....	17
6.2.2 使用服务 .....	17
7 移动电子邮件传输协议 .....	18
附录 A （资料性附录） 支持多样服务环境的因特网电子邮件 (Lemonade) .....	19
A.1 介绍 .....	19
A.2 邮件前转 (Forward without Download) .....	19
A.2.1 消息发送综述 .....	19
A.2.2 传统策略 .....	19
A.2.3 分步描述 .....	20
A.2.4 当票 (pawn-tickets) 机制的安全考虑 .....	27
A.2.5 文件副本拷贝 (file carbon copy) 问题 .....	27

A.2.6 \$Forwarded IMAP 关键字注册.....	27
A.3 消息递交 .....	28
A.3.1 流水线操作.....	28
A.3.2 支持 DSN .....	28
A.3.3 消息大小声明.....	28
A.3.4 支持增强状态码 Enhanced Status Code .....	28
A.3.5 传输层安全 TLS (Transport Layer Security) .....	28
A.4 快同步 .....	28
A.5 附加的 IMAP 扩展 .....	28
A.6 安全性考虑 .....	29
A.6.1 递交的消息的加密保护.....	29
A.6.2 传输层安全 TLS (Transport Layer Security) .....	29
参考文献 .....	30

## 前 言

本技术报告主要参考OMA移动电子邮件需求文档（OMA-RD-Mobile\_Email-V1\_0-20051018-C）、OMA移动电子邮件架构文档（OMA-AD-Mobile\_Email -V1\_0\_0-20070308-D）、OMA移动电子邮件技术规范（OMA-TS-Mobile\_Email -V1\_0-20070110-D）、IETF RFC 4550等标准，并结合国内的具体情况制定的。

本技术报告的附录A是资料性附录。

为适应信息通信业发展对通信标准文件的需要，在信息产业部统一安排下，对于技术尚在发展中，又需要有相应的标准性文件引导其发展的领域，由中国通信标准化协会组织制定“通信标准类技术报告”，推荐有关方面参考采用。有关对本技术报告的建议和意见，向中国通信标准化协会反映。

本技术报告由中国通信标准化协会提出并归口。

本技术报告起草单位：华为技术有限公司、北京邮电大学、中国移动通信集团公司、信息产业部电信研究院

本技术报告主要起草人：王雷、杨健、陈国乔、王丹志、李劼、谢丰、匡晓烜

# 移动电子邮件业务技术要求

## 1 范围

本技术报告规定了移动电子邮件（Mobile Email）的业务描述、功能要求、网络结构和传输协议。  
本技术报告适用于移动电子邮件业务。

## 2 规范性引用文件

下列文件中的条款通过本技术报告的引用而成为本技术报告的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准文件，然而，鼓励根据本技术报告达成协议各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本技术报告。

IETF RFC 2045	多用途邮件扩展第一部分
IETF RFC 2088	IMAP4非同步化报文
IETF RFC 2177	IMAP4 IDLE命令
IETF RFC 2342	IMAP4名字空间
IETF RFC 2821	简单邮件传输协议
IETF RFC 2822	因特网消息格式
IETF RFC 3030	用于传输大二进制MIME消息的SMTP业务扩展
IETF RFC 3207	用于传输层安全之上的SMTP安全的SMTP业务扩展
IETF RFC 3265	会话初始化通知——用于事件通知
IETF RFC 3501	互联网消息接入协议第四版
IETF RFC 4315	互联网消息接入协议——UIDPLUS扩展
IETF RFC 4409	用于邮件的消息呈递
IETF RFC 4467	因特网消息接入协议URLAUTH扩展
IETF RFC 4468	消息递交BURL扩展
IETF RFC 4469	因特网消息接入协议CATENATE扩展
IETF RFC 4551	用于条件存储操作或者快速标记更改重新同步的IMAP扩展
OMA	客户端配置1.1版本
OMA	设备管理1.2版本
OMA	全球许可管理1.0版本
OMA	呈现1.0版本
OMA	标准转码接口1.0版本
OMA	用户代理能力集2.0版本

## 3 术语、定义和缩略语

### 3.1 术语和定义

下列定义适用于本技术报告。

#### 3.1.1

附件 attachment

## YDB 028—2009

消息体中一个特殊的体部分。附件可被用于在线显示或者以指定的方式呈现，如，图形或字处理文件。

## 3.1.2

**授权 authorize**

"authorization"是赋予一个系统实体的权力，允许这个实体访问某个系统资源。"authorization process"是授予这种权力的过程。"authorize"意味着授出这种权利。如IETF RFC 2828所定义。

## 3.1.3

**体 body**

在头后面，包含一个或多个部分（part）。一个体可能包含一些或者所有以下的结合：

如IETF RFC 2822所定义的普通的文本部分；

如IETF RFC 2045所定义的MIME部分，例如：多媒体内容(例如：SMIL、HTML)和其他的附件(例如：word文档，PDF，GIF，JPEG等等……)。

## 3.1.4

**电子邮件帐号 email account**

电子邮件帐号是一系列规则和证书的集合，它允许用户访问和管理电子邮件的用户参数和电子邮件消息。

## 3.1.5

**电子邮件数据 email data**

电子邮件数据是一个所有与电子邮件消息相关的数据的综述；它包括电子邮件消息，电子邮件事件，过滤规则，和用户参数。

## 3.1.6

**邮件事件 email events/event**

有诸如阅读、移动、删除一封邮件等操作导致的邮件状态改变（如，已读/未读，已标记，已删除等……）一封新邮件的到达同样被看作一个事件。

## 3.1.7

**邮件消息 email message**

一个数据序列包含一个头并且可能包含一个体及元数据，其中头和体的格式遵循IETF RFC 2822的描述。

## 3.1.8

**邮件会话 email session**

电子邮件客户和电子邮件服务器之间的会话，在这两个实体之间对收件箱的操作进行更新。本技术报告的该会话存在于移动电子邮件服务器和电子邮件服务器之间。

## 3.1.9

**邮件服务器 email server**

一般来说，电子邮件服务器是提供给用户的电子邮件存储访问的组件（邮件存储）以及提供给用户的电子邮件递交方式的组件(消息传输代理)。在具体实现的时候，电子邮件服务器可能是和移动电子邮件服务器捆绑在一起，或者作为一个单独的组件。

## 3.1.10

**事件过滤 event filters**

决定哪一个电子邮件事件会引起通知(例如：收到新邮件，读取，删除)的过滤规则。

## 3.1.11

**过滤规则 filtering rules**



一组动作或条件的集合,其条件用于决定一封新邮件或邮件通知是否应该从客户端发往服务器或由服务器发往客户端。

### 3.1.12

#### 头 header

由IETF RFC 2822 “Internet Message Format”的定义。以“域名:域体”格式组成的若干行有序字符。

### 3.1.13

#### 移动电子邮件队列 MEM alignment

一种过程和机制,通过这种过程和机制移动电子邮件客户端更新到移动电子邮件服务器的合适的视图,移动电子邮件服务器更新到移动电子邮件客户端的合适的视图。这里合适的视图意味着所对应的数据(根据配置和用户参数被过滤的)的一个子集。

### 3.1.14

#### 移动电子邮件协议 MEM protocol

允许移动电子邮件客户端和移动电子邮件服务器之间交换消息的协议,包括对移动操作的控制、通知等等。

### 3.1.15

#### 移动电子邮件代理 MEM proxy

提供移动邮件代理服务的代理。它允许移动电子邮件协议在移动电子邮件服务器前端通过防火墙。这个代理的功能是:当电子邮件服务器处于不同的部署模型中的时候,允许移动电子邮件服务器处在同一个域。这样就减轻了可能加在移动电子邮件服务器实现上的加密以及其他的安全限制。

### 3.1.16

#### 移动电子邮件会话 MEM session

处于移动电子邮件客户端和移动电子邮件服务器之间的会话,反映数据(已作为电子邮件会话的一部分被交换)的状态。

### 3.1.17

#### 元数据 meta data

由服务器应用的机器生成的(Machine-generated)属性,在传递的时候出现在头域中。例如,包含重发头域,消息内容(语音邮件、电子邮件、MMS、SMS)和处理结果。

### 3.1.18

#### 移动电子邮件 mobile email

一种用于促进移动终端,在端到端应用层处理电子邮件事务(发送、提取、通知等)的技术。

### 3.1.19

#### 其它移动引擎 other mobile enabler

被移动电子邮件服务器或者移动电子邮件客户端使用的提供附加的移动电子邮件功能(比如:带外通知,参数配置/设备管理等等)的一切引擎。

### 3.1.20

#### 带外通知 out-band notification

从服务器到客户端的关于电子邮件服务器事件的通知,由通道(例如:SMS, MMS, WAP Push, SIP Push, 等等)而不是移动电子邮件协议传输。

### 3.1.21

#### 服务器到客户端的通知 server to client notification

服务器通知客户端状态改变的手段,例如,一份新的邮件到达服务器。

### 3.1.22

YDB 028—2009

挂起和恢复 suspend and resume

一种允许在数据交换时被自动或非自动的挂起/暂停的地方恢复机制，而不要求发送此前交换的大多数数据。

3. 1. 23

处理规则 processing rules

应用于收发时的动作或条件，包括：垃圾邮件拦截，过滤规则病毒处理，附件移除。

3. 1. 24

视图过滤 view filters

决定哪个电子邮件消息对移动电子邮件客户端是不可见的。被规定的不可见得电子邮件消息被移动电子邮件服务器隐藏。

3. 2 缩略语

下列缩略语适用于本技术报告。

CP	Client Provisioning	客户端配置
DS	Data Synchronization	数据同步
DSN	Delivery Status Notification	传递状态通知
EMN	Email Notification	电子邮件通知
ESMTP	Extension SMTP	SMTP 扩展
GPM	Global Permission Management	全球许可管理
IETF	Internet Engineering Task Force	互联网工程任务组
IMAP4	Internet Message Access Protocol 4	因特网消息接入协议 4
MEM	Mobile Email Enabler	移动电子邮件引擎
MIME	Multipurpose Internet Mail Extensions	多用途因特网邮件扩展
MMS	Multimedia Messaging Service	多媒体消息业务
MUA	Mail User Agent	邮件用户代理
OMA	Open Mobile Alliance	开放移动联盟
RD	Requirement Document	需求文档
SAS	Server Alerted Sync	服务通告同步
SIP	Session Initiation Protocol	会话初始化协议
SMIL	Synchronous Multimedia Integration Language	同步多媒体整合语言
SMS	Short Message Service	短消息业务
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
STI	Standard Transcoding Interface	标准转码接口
TLS	Transport Layer Security	传输层安全
UAProf	User Agent Profile	用户代理描述
UDP	User Datagram Protocol	用户数据报协议
WAP	Wireless Application Protocol	无线应用协议
WDP	Wireless Datagram Protocol	无线数据报协议

4 业务描述

电子邮件是因特网上应用最广泛、使用人数最多的一个系统。电子邮件已经成为全球信息联络的重要工具。也是因特网得以如此快速普及推广的一个重要原因。电子邮件使用方便、传递迅速、费用低廉，不仅可以传送文字信息，还可以附上声音和图像。



移动电子邮件（Mobile Email）是一种用于移动终端的电子邮件技术。使用移动电子邮件技术，用户可以不受位置和移动的限制，随时随地的接收和发送电子邮件。并且，移动电子邮件可以同终端的其它应用相结合，为用户提供实用的应用。例如，移动电子邮件可以同终端的日程提醒相结合，用户设定提醒条件（如开会），在满足提醒条件时（如会议开始前十分钟），向相关人员（如与会人）的终端发送电子邮件提醒（还可以携带会议资料）。

移动电子邮件技术具有迅速、便捷的好处。通过该技术达到在用户看来移动终端能够以非长时间联网的方式接入电子邮件服务器，并能完成下述操作：

- a) 当一封电子邮件到达企业的邮件服务器时，应当及时、安全的通知终端上的客户端有一封电子邮件到达。基于用户的设置，终端可以显示电子邮件通知，提示用户有新邮件到达是否提取。也可以在收到电子邮件通知后不显示给用户，而是终端自动提取新邮件或新邮件的一部分（例如，信头、开头的若干字节，或者是不含附件的邮件正文）。带给移动用户的体验应该能同桌面电子邮件系统相媲美。
- b) 用户以适合其终端的方式下载和浏览附件。
- c) 用户在移动终端创建了一条电子邮件并选择发送时，这封邮件应该立即由公司内部的电子邮件服务器发往目标地址（不能是其它的服务器，例如运营商提供的SMTP服务器）。
- d) 公司邮件服务器中的用户信箱应该与用户移动终端上电子邮件客户端的状态保持一致。例如，用户在终端本地删除一封电子邮件或者将邮件从一个文件夹移到另一个文件夹时，公司服务器上应该反映出相应的操作。
- e) 针对新邮件到达企业电子邮件服务器后发送到移动客户端的过程，用户可以在移动终端上设定过滤规则。
- f) 根据移动用户所使用的网络/服务提供商情况（如基础网络的技术、漫游、费用等）不同，他/她可以更改移动电子邮件的设置以适当的满足下述要求：
  - 1) 使用现有的消息机制（例如，SMS，MMS，Push）以安全的方式通知新邮件的到达（也有可能是别的事件）：
    - a) 在数据会话中以自动的方式，安全的提取邮件；
    - b) 在数据会话中以手动的方式，安全的提取邮件；
    - c) 安全的浏览接入方式（例如，WAP，Web，Voice）；
    - d) 用户可以使用OTA的方式同步他的电子邮件，还可以直接通过蓝牙、红外LAN等方式直接同PC端同步。
  - 2) 电子邮件服务器可以提供一种划分电子邮件安全级别的操作方法：在电子邮件服务器中记录各安全级别所对应的操作权限；电子邮件服务器确定、记录邮件的安全级别并根据所对应的操作权限控制用户的操作（如：完全操作权限、密码保护、不允许下载等）。

## 5 功能要求

### 5.1 接收邮件

一封电子邮件到达邮件服务器。通过安全的通知方式，及时的通知终端上的客户端该新邮件的到达。我们将此称为一个事件（event）。基于用户的参数选择，该事件对用户或客户端可用，即，一旦安全的鉴权，接入新邮件或按需获取其一部分（如，信头、开头的若干千字节，不含附件的整个体或整封邮件）。带给移动用户的体验应该是不可察觉时延或者至少是能同桌面电子邮件相媲美。事件可以包括发送一部分或者所有的邮件，在这种情况下，访问无需分步进行。另外，客户端可以接收邮件事件或主动获取。

流程如下：

## YDB 028—2009

- a) 电子邮件到达电子邮件服务器；
- b) 电子邮件服务器根据用户事先的设置生成电子邮件通知；
- c) 电子邮件通知对移动客户端可用，包括：通知送达、邮件客户端的接入可用；
- d) 客户端检查用户的参数配置；
- e) 客户端按照设置下载电子邮件；
- f) 用户可以阅读电子邮件。

## 5.2 接收电子邮件通知

可以用一种及时并且安全的方式将事件通知终端上的客户端。基于用户的参数设置（例如，服务器上的删除或移动操作在客户端得以镜像，服务器收件箱中建立的文件夹结构能够在客户端呈现……），事件对用户可用，或者客户端反映出该事件。移动用户察觉不到延时或者至少是能同桌面电子邮件相媲美。

流程如下：

- a) 电子邮件服务器上有事件发生，例如，一封新邮件到达；
- b) 电子邮件服务器根据用户预先设置的信息格式，针对要发送给终端的新电子邮件生成邮件情况信息；
- c) 电子邮件服务器将生成的邮件情况信息发送给终端（通过电子邮件通知发送）；
- d) 终端的客户端按照预定格式解析收到的邮件情况信息；
- e) 终端的客户端根据所获得的用户电子邮件通知接收策略；
- f) 终端的客户端根据所获得的用户电子邮件通知接收策略控制对电子邮件通知的处理；
- g) 用户可以看到移动电子邮件情况信息。

## 5.3 接收大邮件

由于终端设备的能力限制，在接收大邮件时，需要根据用户设置的门限大小进行相应的处理，接收小于改门限的电子邮件，对大于该门限的电子邮件进行相应处理（如仅下载电子邮件的头）。

## ● 流程 1 如下：

- a) 用户在客户端上设置一个允许接收邮件容量的最大值，即容量门限；
- b) 当用户请求收取邮件或者是服务器要求用户收取邮件时，服务器向客户端发送包含邮件容量信息的邮件通知；
- c) 客户端对接收到的邮件通知进行解析，获取邮件容量信息；
- d) 客户端判断邮件容量信息，判断需要接收的邮件的容量是否大于容量门限，若大于容量门限，则可以进行以下两种处理方式：
- e) 拒绝该邮件的下载或仅下载该邮件的邮件头，即仅下载该邮件的摘要信息，例如发件人，发件时间等信息。

## ● 可选流程 2 如下：

- a) 用户在客户端上设置一个允许接收邮件容量的最大值，即容量门限；
- b) 客户端将用户设置的容量门限发送至服务器；
- c) 当服务器接收到新的邮件时，首先检测接收到的新邮件的容量是否大于容量门限，若小于容量门限，则允许向客户端发送该邮件的邮件通知，若大于容量门限，则不向客户端发送该邮件的邮件通知。

## 5.4 阅读邮件附件

用户以适合其设备的方式查看附件。

流程如下：

- a) 服务器收到带有附件的电子邮件；

- b) 电子邮件遵照 5.1 收取流程下载电子邮件，但是遵照 5.1，附件并没有下载到客户端；
- c) 用户选择查看附件；
- d) 客户端要求下载附件；
- e) 电子邮件服务器根据终端能力对附件进行内容适配；
- f) 客户端下载附件；
- g) 用户查看附件。

## 5.5 发送邮件

一封电子邮件被创建后，一旦选择发送电子邮件，这封电子邮件可以立即从用户的邮件服务器以安全的方式发送。移动邮件用户创建一封移动电邮，可以包括编辑消息，附加多个文件，重编辑任何已存的草稿等等诸如此类的操作。在选择发送电子邮件后，这封电子邮件将被上传到用户的电邮服务器并且立刻以一种安全的方式由服务器发出。

流程

- a) 用户在终端上编辑完成一封电子邮件；
- b) 用户选择发送电子邮件；
- c) 客户端连接电子邮件服务器并上传电子邮件；
- d) 电子邮件被发送到电子邮件服务器；
- e) 电子邮件可被保存在已发送文件夹中；
- f) 电子邮件服务器根据用户实现的设置发送文件夹中的电子邮件。

## 5.6 改变过滤规则

在移动时，用户可以改变过滤规则。这些过滤规则指定了何种邮件，在何时，以何种方式到达电邮服务器或者电邮服务器的事件必须被反映或呈报给移动电邮客户端。

流程如下：

- a) 用户决定更改过滤规则；
- b) 新的规则传送到电子邮件服务器。

## 5.7 客户端之间的数据同步

用户可以同步他的电子邮件，通过与另一个电脑或客户端连接（蓝芽，红外，LAN直连）实现。

流程如下：

- a) 第一个客户端与电子邮件服务器同步；
- b) 用户选择第二个客户端对第一个客户端数据同步；
- c) 第二个客户端与电子邮件服务器数据同步。

## 5.8 带有附件的邮件

一封带有附件的电子邮件到达用户的邮件服务器。因为这封邮件具有一个附件，基于用户的参数选择，服务器可以传递该邮件的所有部分或仅这封邮件的文本部分。

流程如下：

- a) 用户的收件箱中接收到一封带有附件的电子邮件；
- b) 邮件服务器，基于用户的设置，仅下载消息的头。

## 5.9 在不下载附件的情况下转发邮件

● 流程 1 如下：

- a) 用户 A 的收件箱中接收到一封带有附件的电子邮件；
- b) 邮件服务器，基于用户 A 的设置，仅向 A 的客户端传递消息的头；
- c) 用户 A 在没有下载附件和整个文本的情况下，将邮件转发给了用户 B；
- d) 邮件服务器将该带有附件的邮件转发给了用户 B。



- 流程 2 如下：

- a) 客户端获取邮件标识信息；
- b) 客户端设置邮件转发信息并同步到移动电子邮件服务器；
- c) 移动电子邮件服务器根据邮件转发信息将指定邮件整合为转发邮件并发送。

## 5.10 配置电子邮件帐号

用户为了在移动终端正常使用电子邮件，需要配置移动电子邮件客户端。用户还可能希望对电子邮件帐号进行配置，以完成如接入另外的邮件帐户并且合并从不同帐户收到的消息，这些消息是保留在邮件服务器还是删除的功能。

- 流程 1 如下：

- a) 用户选择配置客户端；
- b) 用户输入其邮件地址和用于接入帐号的鉴权信息；
- c) 客户端根据用户输入的电子邮件地址获取所述电子邮件地址中的域名标识；
- d) 客户端将包含所述域名标识的查询请求发送至移动邮件服务器；
- e) 移动邮件服务器根据查询请求查询业务参数（包括电子邮件传输协议参数、接收服务器参数、发送服务器参数），并将所述业务参数反馈客户端；
- f) 客户端根据查询到的业务参数对客户端进行配置。

- 流程 2 如下：

- a) 用户激活终端上的移动电子邮件客户端；
- b) 用户选择配置移动电子邮件客户端；
- c) 用户提供必要的鉴权信息以接入电子邮件帐号；
- d) 用户进行设置；
- e) 电子邮件服务器鉴权并通知用户设置完成。

## 5.11 回复邮件

一个已经将他的移动电邮客户端配置为显示来自不同帐户的用户，他希望针对某条已显示的消息发送一条回复消息。当创建该条回复消息时，客户端应该提供用户选择回复消息中“from”域的能力。

流程如下：

- a) 用户激活终端上的电子邮件客户端；
- b) 用户浏览收件箱中的消息并选择其中一条消息查看；
- c) 用户选择回复消息；
- d) 客户端生成一条新消息供用户编辑；
- e) 客户端显示当前帐户对应的“from”域；
- f) 用户可以根据自己拥有的多个帐户，选择一个“from”域；
- g) 编辑完全后，用户选择发送这条回复消息；
- h) 电子邮件服务器接收到这条回复消息并发送到目的地址。

## 6 网络结构

### 6.1 架构

移动电子邮件体系架构如图1所示。

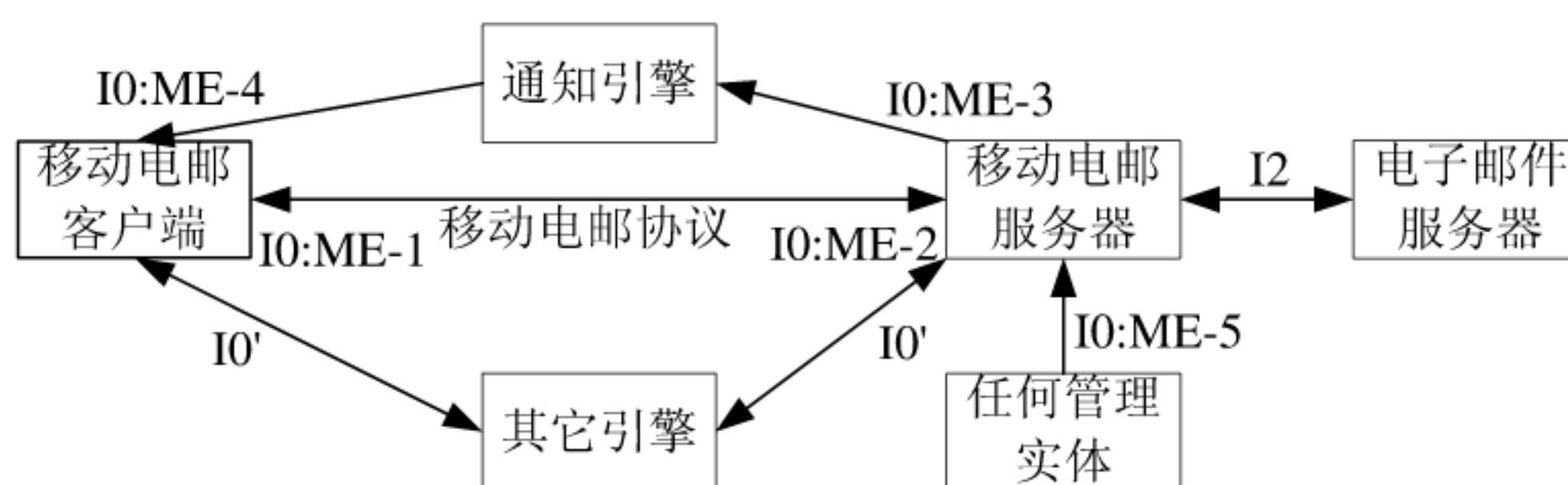


图1 移动电子邮件体系架构

为了描述简单，图中把所有的外部引擎集中到了一个单独的逻辑组件，这幅图描绘了一个引擎集以及他们各自的接口IO'。

### 6.1.1 组件

以下组件对移动电子邮件引擎的运行是必须的：

- 移动电子邮件客户端：它的任务和客户侧功能在中详细的讨论。
- 移动电子邮件服务器：它的任务和服务器侧功能在中详细的讨论。

电子邮件服务器组件实现了存储，接入和管理电子邮件所需要以及任何关于用户参数选择或设定的功能。实现的时候电子邮件服务器和移动电子邮件服务器可能会捆绑在一起。电子邮件服务器不在移动电子邮件引擎的范围内。

以下组件是可选的：

- 通知引擎组件：实现了移动电子邮件引擎的通知功能。

用于通知的消息引擎，这里通知不是通过移动电子邮件协议传送，而是通过其它的渠道，这些渠道可能包括：

- 1) SMS：包括按照EMN方式的SMS或者WAP WDP。
- 2) MMS。
- 3) WAP Push。
- 4) 附加的通知，像SIP push(如IETF RFC 3265所描述的SIP NOTIFY)或者UDP也可能被考虑到。
- b) 任何管理实体：实现了管理移动电邮服务器配置所需要的功能。任何管理实体不在移动电子邮件引擎的范围内。
- c) 其它引擎：是一个占位组件，它表达了任何其他的能够增强OMA 移动电子邮件引擎功能和可用性的组件。其它引擎不在移动电子邮件引擎的范围内。

OMA移动电子邮件体系结构定义了一系列的其它引擎，为了增强有特性的业务配置，每一个其它引擎可能都要被另外配置。哪一个附加的引擎需要配置取决于服务提供商。这里的列表包括的是那些已经被明确提到的可能作为候选的其它引擎。独立的业务部署可以利用任何其它引擎或者技术，也包括下面没有明确包含的，只要它们不带来和移动电子邮件协同工作的故障。

- OMA DM或者OMA CP支持通过空中接口将移动电子邮件客户端安装到设备上，支持移动电子邮件客户端的设置和撤回，如OMA客户端配置1.1版本和OMA设备管理1.2版本中所描述。
- OMA STI和UAProf支持电子邮件消息(消息体和附件)部分的代码转换。如OMA标准转码接口1.0版本和OMA用户代理能力集2.0版本中所描述。
- OMA PAG，移动电子邮件服务器可以根据从PAG引擎中获取的移动终端的状态信息处理电子邮件事件。OMA呈现1.0版本中所描述。
- GPM，如OMA全球许可管理1.0版本所描述，当事人的设置正在通过ME-5被管理的时候，保护它的隐私。为了执行服务提供商的各种各样的策略，非核心的功能可以让其它引擎提供。

- e) 以流量或者其它合适的成本方式计费。
- f) 隐私保护和垃圾邮件防护。

注意：这些策略可以发生在任何一个接口上面(例如：IO:ME-1, 2, 3, 4, 5 和IO')，但是具体的策略不在本技术报告的范围之内。

## 6.1.2 接口

### 6.1.2.1 接口定义

本技术报告的移动电子邮件架构定义了很多接口，他们允许各种组件之间互相通信。所有的这些接口都表示在了图1中，图中的箭头指明了接口的方向：单方向的箭头表示单方向的接口(只能支持发送或接收数据之一)，双方向的箭头表示双向的接口(同时支持收发数据)。确定的接口都有：

- a) IO:ME-1: 移动电子邮件客户端接口, 通过移动电子邮件协议与移动电子邮件服务器交互。
- b) IO:ME-2: 移动电子邮件服务器 接口, 通过移动电子邮件协议与移动电子邮件客户端交互。
- c) IO:ME-3: 通知接口, 使移动电子邮件服务器生成服务器至客户端通知。
- d) IO:ME-4: 通知接口, 使移动电子邮件客户端接收服务器至客户端通知。
- e) IO:ME-5: 用来管理 移动电子邮件服务器设置的接口。
- f) IO': 向其它引擎(比如: DM, CP, 消息)发送或从中接收数据的接口。IO' 接口不在移动电子邮件引擎的范围内, 它们由所引用的引擎提供。
- g) I2: 移动电子邮件服务器和电子邮件服务器之间的接口。I2 接口不在移动电子邮件引擎的范围内。

### 6.1.2.2 接口使用

这一节描述为了提供移动电子邮件业务, 什么协议和通知利用这些确定的接口。以下章节主要关于:

- a) 协议: 电子邮件和移动电子邮件协议;
- b) 通知: 带内和带外通知。

#### 6.1.2.2.1 协议

##### 6.1.2.2.1.1 电子邮件协议

电子邮件协议用在I2接口上用来提供移动电子邮件服务器和电子邮件服务器之间的通信, 由于电子邮件服务器和 I2 接口不在 OMA 移动电子邮件引擎的描述范围之内, 电子邮件协议也不在其中, 因此, 这里不提供它的准确细节。然而, 可以有这样一个方针: 任何能够提供电子邮件交换的已有协议, 都可以被用作电子邮件协议; 举其中几例: SMTP, IMAP, POP等等。

当I2接口在具体实现之内的话, 电子邮件协议就不可用了。

##### 6.1.2.2.1.2 移动电子邮件协议

一般地, 移动电子邮件客户端和移动电子邮件服务器使用移动电子邮件协议在IO:ME-1和IO:ME-2之间通信, 然而这个架构模型中使用IO' 接口也能达到这个目标。只有移动电子邮件客户端是联机状态时, 移动电子邮件协议才能使用: 移动电子邮件协议 传递所有的电子邮件数据以及移动电子邮件客户端和移动电子邮件服务器之间的带内通知。移动电子邮件引擎专注于处理移动电子邮件客户端和移动电子邮件服务器之间的交互。移动电子邮件服务器和电子邮件服务器之间的交互不在本技术报告的讨论范围之内。

移动电子邮件体系结构定义了移动电子邮件协议的职责。由于移动电子邮件协议是移动电子邮件引擎的核心, 它有很广泛的职责。所以在下面的章节里将分别讨论:

- 移动电子邮件队列: 将移动电子邮件客户端/服务器更新到适合另一方的视图;
- 管理并使用过滤规则: 配置和维护过滤规则;
- 管理并使用设置和参数: 配置和维护各种参数;
- 媒体转换: 执行各种类型的媒体转换。



## a) 移动电子邮件队列

一般来说,移动电子邮件队列包括在移动电子邮件客户端和电子邮件服务器之间通过移动邮件服务器双向地排列,读取和升级电子邮件事件的机制:

- 在移动电子邮件服务器上反映出客户端侧的电子邮件事件。
- 根据设置/过滤规则,在移动电子邮件客户端上反映出服务器侧的电子邮件事件。

为了管理连通性,优化带宽利用,覆盖附加的配置模型以及增强安全性,移动电子邮件队列还包括以下机制:

- 1) 支持基于电子邮件部件(体、地址域和附件)的在移动电子邮件服务器上的远程消息整合。这里的电子邮件部件可能还没有被下载,或者有一些已经在本地生成了,或者被下载和编辑了。支持只下载体部件的不同部分(例如:地址域)似乎更加合理。
- 2) 在所有的数据交换中优化带宽利用,包括(但不仅仅限于):
  - 利用数据压缩的数据交换;
  - 减少往返传输数;
  - 使在挂起和重新开始之间减少数据交换冗余。
- 3) 对电子邮件服务器和移动电子邮件客户端之间交换的电子邮件数据进行加密。
  - 即使移动电子邮件服务器布置在电子邮件服务域外,电子邮件数据仍然应该一直保持加密;
  - 一旦通知携带的消息值得保护,也应该对它进行加密。
- 4) 允许移动电子邮件客户端和移动电子邮件服务器之间的结构和配置以带内或带外的方式交换:
  - 服务器到客户端:例如:服务器ID,账户名字,策略,服务器性能,等等;
  - 客户端到服务器:例如:过滤规则,休假公告,通知频道客户端性能,等等。
- 5) 支持不同的部署模型。在固网或移动网络中,当有防火墙或其他中间媒介存在的时候,移动电子邮件必须可用。
- 6) 保证电子邮件服务器和移动电子邮件客户端之间交换的电子邮件数据的完整性。
- 7) 移动电子邮件客户端和移动电子邮件服务器之间的双向鉴权机制。
- 8) 允许移动电子邮件客户端通过移动电子邮件服务器向电子邮件服务器发送召回请求的机制。
- 9) 标记移动电子邮件客户端和移动电子邮件服务器的机制。
- 10) 允许移动电子邮件客户端在离线、网络时断时续、或者移动设备有功能限制的状态下工作:
  - 存储电子邮件和客户端电子邮件事件;
  - 监测网络可用性;
  - 当网络连接可用的时候发送电子邮件和客户端电子邮件事件;
  - 恢复和重续中断的发送和接收进程。
- 11) 支持多账户的功能,比如:
  - 逐个地配置多个邮件账户;
  - 从多个邮件账户接收电子邮件;
  - 从选中的邮件账户发送邮件。

注:可以是用户手动选择,也可以是客户端或服务器从用户配置的多个邮件账户中自动选择。

移动电子邮件队列依靠通知传递电子邮件事件。因此,移动电子邮件协议必须包括带内外通知并且确保如下几条:

- 最小化电子邮件服务器上的电子邮件事件在移动电子邮件客户端上反映出来时的时延。
- 避免来自移动电子邮件客户端的不必要请求(包括探测)。
- 移动电子邮件客户端能够定义并且处理延迟的通知,并且能够妥善处理丢失的通知。

- 带外通知被指明为网络并且通过寻址绑定到各种各样的独立的通知信道(例如: SMS、WAP Push、SIP 通知等等)独立地传输。

b) 过滤规则的管理和使用

移动电子邮件协议描述了过滤规则的获得, 生成, 升级和删除功能。

c) Setting 和 Preferences的管理和使用

移动电子邮件协议描述了设置和参数选择的获得, 生成, 升级和删除功能。

d) 媒体转换

移动电子邮件客户端能够请求来自移动电子邮件服务器的媒体转换。涉及到媒体转换的移动电子邮件协议功能包括:

1) 当从电子邮件服务器获得电子邮件消息部分的时候, 允许移动电子邮件客户端请求来自移动电子邮件服务器的消息部分(包括附件)的媒体转换(包括码型转换)。

- 移动电子邮件客户端可以请求到一个特定格式或大小的转换。
- 移动电子邮件客户端可以请求到一个服务器选定的格式或大小的转换, 在这里移动电子邮件服务器根据具体情况(例如: 客户端能力, 用户参数)决定格式或大小。

移动电子邮件服务器收到移动电子邮件客户端发送的邮件请求后可获取终端的能力集信息(例如: 客户端能力, 用户参数, 可以通过OMA UAProf获取), 然后将终端的能力集信息和要适配的邮件发送给终端适配服务器(可以通过OMA STI接口)进行媒体转换后发送给移动电子邮件客户端。

2) 媒体转换并不改变电子邮件服务器中的消息内容。

3) 可选地, 电子邮件服务器还可以备份转换后的媒体数据, 如果移动电子邮件服务器根据邮件标识发现要进行媒体转换的邮件存在转换备份, 则可以直接将转换备份发送给移动电子邮件客户端。

#### 6.1.2.2.2 通知

通知总是从服务器发往客户端。通知用来从移动电子邮件服务器向移动电子邮件客户端传递消息, 而不需要移动电子邮件客户端事先探询改变。基于移动电子邮件客户端的连接状态, 定义了两种通知:

1、带内通知;

2、带外通知。

带内通知和带外通知在一个邮箱内不能共存。

两种通知都遵从过滤规则。

服务器还可以结合终端的presence状态信息(如是否开机、是否在线、是否设置免打扰等)选择合适的通知方式向电子邮件客户端传递电子邮件事件。

##### 6.1.2.2.2.1 带内通知

只要移动电子邮件客户端在线, 移动电子邮件服务器就会用带内通知告知移动电子邮件客户端相关的电子邮件事件。带内通知利用移动电子邮件协议进行传输。

带内通知必须携带维持移动电子邮件队列所必需的所有信息。

移动电子邮件客户端必须处理并且行使带内通知中的信息。

##### 6.1.2.2.2.2 带外通知

当移动电子邮件客户端离线时, 基于用户设定和服务提供商策略, 移动电子邮件服务器能够使用带外通知通知移动电子邮件客户端相关的电子邮件事件。通常, 带外通知使用IO:ME-3和IO:ME-4接口通过带外通知引擎组件传输。

当移动电子邮件客户端离线的时候, 并不要求携带所有维持移动电子邮件队列的必要信息。包含在带外通知中的细节取决于移动电子邮件服务器的实现方式。如果目标是将带外通知中的数据量最小化, 那么所有的细节都可以被省去, 只需要指明一个电子邮件事件发生了。如果目标是在移动电子邮件客户

端连接状态保存,则可以包含关于电子邮件事件的细节信息。另外,移动电子邮件服务器实现也可以提供基本的流控:缓存电子邮件事件并且把它们分批地发送出去,而不是一个接一个地向客户端发送。例如:一个带外通知可以包括很多的电子邮件事件。无论何种情况,如果敏感信息(例如:通知携带的内容需要保护)包含在了带外通知中,它就应该被加密。

### 6.1.3 移动电子邮件客户端

为了实现移动电子邮件引擎特性,移动电子邮件客户端负责实现客户端的功能。

客户侧的功能和移动电子邮件客户端可以被分解并且分配到不同的子组件。然而,这种分解不在本技术报告的讨论范围之内:本技术报告将移动电子邮件客户端视为一个整体。

客户侧的功能包括(但不仅限于)提供如下特性:

- a) 连接其他组件的接口;
- b) 用户接口;
- c) 会话管理;
- d) 电子邮件数据管理;
- e) 事件处理。

#### 6.1.3.1 连接其他组件的接口

所有的接口都定义在了接口中。

移动电子邮件 客户端能提供如下接口:

- a) IO:ME-1 - 用于 移动电子邮件协议, 见移动电子邮件协议。
- b) IO:ME-4 - 用于带外通知, 见通知。
- c) IO' - 用于其它引擎。

#### 6.1.3.2 用户接口

用户接口使终端用户能够使用移动电子邮件服务,这里的 service 指的是收、发和组织邮件。

本技术报告没有提供任何关于用户接口的指导方针,因此,用户接口取决于实现方式。

#### 6.1.3.3 会话管理

移动电子邮件客户端使用移动电子邮件 会话与移动电子邮件服务器进行通信。移动电子邮件会话是使用移动电子邮件协议在IO:ME-1和IO:ME-2之间建立的。关于这些会话,移动电子邮件客户端的职责是:

- a) 建立和维护移动电子邮件会话(包括挂起和恢复);
- b) 处理间歇的连接;
- c) 会话过程中的安全传输。

#### 6.1.3.4 电子邮件 Data 管理

一般来讲,移动电子邮件客户端的电子邮件数据管理是指提供和实施如下的特性和功能:允许查看,生成,更新,处理,存储和撤除本地或远程的电子邮件数据。关于电子邮件数据管理,移动电子邮件客户端的职责包括:

- a) 客户端对管理用户参数的支持。
- b) 客户端对本地行为的实现。
- c) 支持电子邮件使用的机制,包括:
  - 1) 读取;
  - 2) 写作;
  - 3) 保存;
  - 4) 发送;
  - 5) 在已下载或未下载的情况下转发或回复。



## 6) 消息删除特性:

- 本地删除: 从移动电子邮件客户端的角度删除电子邮件消息, 在电子邮件服务器保留。可能要向移动电子邮件服务器传送一些信息。
- 附件的本地删除, 从客户端删除附件, 当正在查看时仍可以从电子邮件服务器再次下载附件。
- 远程删除: 从移动电子邮件客户端和电子邮件服务器都将消息删除的能力。

7) 管理下载特性, (例如: 只下载头, 只下载特定大小的数据, 只下载体、选中的附件、或者更多的附件)。

8) 利用移动电子邮件服务器提供的估计完成下载电子邮件消息和它的附件所需要的时间。

9) 允许用户生成, 更新, 删除, 动态或非动态地自动回复消息, 并将其上传到服务器。

## d) 客户端下载和存储用户参数:

- 1) 管理哪一个可访问的消息在移动电子邮件客户端被维护;
- 2) 管理可访问的消息的哪些部分被下载并在客户端维护;
- 3) 这些参数可以由用户配置;
- 4) 加密并保护本地存储的消息。

## e) 客户端安全, 包括:

- 1) 密码保护;
- 2) 本地消息存储加密;
- 3) 本地密钥管理。

**6.1.3.5 事件处理**

移动电子邮件客户端负责处理电子邮件事件。电子邮件事件可能起源于移动电子邮件客户端, 移动电子邮件服务器或者电子邮件服务器。在移动电子邮件客户端在线和脱机状态时对电子邮件事件的处理是不同的, 这些方面在以下章节会讨论。

移动电子邮件服务器还可以结合终端的presence状态信息(如是否开机、是否在线、是否设置免打扰等)对电子邮件事件进行相应处理。

**6.1.3.5.1 移动电子邮件客户端在线时的电子邮件事件**

移动电子邮件客户端要使用移动电子邮件协议向移动电子邮件服务器传递所有的起始于电子邮件事件。

只要移动电子邮件客户端在线, 移动电子邮件服务器就会使用带内通知向移动电子邮件客户端传递电子邮件事件。

移动电子邮件服务器可以将邮箱中所有邮件夹(当前选中的和未选中的邮件夹)中满足过滤规则的电子邮件事件(e.g. 新邮件事件、邮件状态变化事件)通过带内通知发送给移动电子邮件客户端, 以保持客户端和服务端邮箱中邮件的同步。

**6.1.3.5.2 移动电子邮件客户端脱机时的电子邮件事件**

在下次移动电子邮件队列之前, 移动电子邮件客户端可以将所有的始于客户端的电子邮件事件排队。并不要求立即执行移动电子邮件队列。

当移动电子邮件客户端是脱机状态时, 移动电子邮件服务器可以使用带外通知向移动电子邮件客户端传递电子邮件事件。根据带外通知的内容, 移动电子邮件客户端可以选择执行移动电子邮件队列。带外通知可以描述用户邮箱里准确的变化; 这使得移动电子邮件客户端能够在本地应用相应的变化(不必执行移动电子邮件队列), 即使移动电子邮件客户端并没有被要求这样做。另一方面, 可能有些变化在带外通知中没有描述; 因此, 除非执行移动电子邮件队列, 这些变化在本地将不能被应用。由于移动电子

邮件并不被要求立即执行移动电子邮件队列, 所以最好在移动电子邮件客户端检测到带外通知丢失或延迟时, 再执行移动电子邮件队列。

#### 6.1.4 移动电子邮件服务器

移动电子邮件服务器负责实现移动电子邮件引擎服务器侧的功能。

移动电子邮件服务器的主要角色是在电子邮件服务器前端提供这样一个逻辑实体:

- a) 提高电子邮件服务器的性能: 允许移动客户端更高效的接入电子邮件服务器。
- b) 提供到电子邮件服务器的这样的一种接入: 使用的协议不是明确的被移动电子邮件客户端支持。

由于广泛的部署模型, 各种各样的客户端以及电子邮件服务器, 移动电子邮件服务器必须是可配置的, 以支持不同的电子邮件服务器, 安全水平, 和逻辑流。这里的配置还应当考虑到部署模型的各种各样的特性。

服务器侧的功能包括(但不仅仅限于)提供如下特性:

- a) 到其它组件的接口;
- b) 管理接口;
- c) 会话管理;
- d) 电子邮件数据管理;
- e) 事件处理;
- f) 媒体转换。

##### 6.1.4.1 到其他组件的接口

移动电子邮件服务器能提供如下接口:

- a) I0:ME-2 – 用于移动电子邮件协议;
- b) I0:ME-3 – 用于带外通知;
- c) I0:ME-5 – 用于管理的目的;
- d) I2 – 用于电子邮件协议;
- e) I0' – 用于其它引擎。

##### 6.1.4.2 可管理的接口

管理的目的是允许授权的当事人配置或者更新移动电子邮件上的各种设置。为了这个目的, 移动电子邮件体系架构定义了接口: I0:ME-5。

被管理的设置一般都是改变移动电子邮件 服务器自身的行为(移动电子邮件 服务器设置), 或者他们与各种用户设置相关(用户参数, 过滤规则), 这或者是全局的, 也可以是基于每个用户的。

为了安全起见, 管理接口除了管理设定外不应该有它用(例如, 调试, 日志, 计费等等, 不允许使用这个接口)。

##### 6.1.4.3 会话管理

一般的, 移动电子邮件服务器需要管理两种会话: 一个移动电子邮件会话和一个电子邮件会话. 管理更多的会话可能也有必要, 这取决于I0:ME-3, I0:ME-5, 和I0' 的实现选择, 然而, 这些更多的会话的管理还取决于移动电子邮件服务器的实现。移动电子邮件会话是由移动电子邮件客户端建立并维护的。只要有需要, 移动电子邮件客户端就会试图使用I0:ME-1和I0:ME-2接口不时的建立移动电子邮件会话。

移动电子邮件服务器和电子邮件服务器之间使用电子邮件会话通信。移动电子邮件服务器负责建立和维护电子邮件会话。电子邮件会话是在I2接口上建立的. 由于I2 接口不在本技术报告讨论范围之内, 这里不能提供关于I2的细节描述。然而作为一个指导方针: 一般对于每一个移动电子邮件会话, 移动电子邮件服务器需要维持一个电子邮件会话。(个别的移动电子邮件服务器实现可能突破这种局限, 然而不在本技术报告讨论范围之内)。

移动电子邮件服务器的职责对移动电子邮件会话和电子邮件会话是通用的，这些职责包括：

- a) 对事件接收者的地址解析；
- b) 提供多个移动电子邮件客户端同时会话(包括挂起和续接)；
- c) 提供一个邮箱和不同移动电子邮件客户端之间的同时的多会话；
- d) 提供从一个移动电子邮件客户端到不同邮箱的同时的多会话；
- e) 维持到电子邮件服务器会话的连接性即使移动电子邮件客户端的连接性是断续的；  
维持会话状态并且在会话重新连接后更新客户端；
- f) 应付可能的连接缺乏(例如：排队和存储事件)；
- g) 处理可能的连接缺乏(比如：排队，或者存储事件)。

#### 6.1.4.4 电子邮件数据管理

对于移动电子邮件服务器, 电子邮件数据的管理一般是指提供和执行如下的特性和功能：允许在移动电子邮件客户端和它们的电子邮件服务器之间收回，处理，存储，移除电子邮件数据。关于电子邮件数据的管理，移动电子邮件服务器的职责包括：

- a) 维护消息内容的安全性，在移动电子邮件客户端和电子邮件服务器之间信息的交互。
  - 1) 电子邮件服务器的鉴权；
  - 2) 移动电子邮件客户端的鉴权和授权；
  - 3) 递交的消息的(客户端)发起者的鉴权和授权。
- b) 将用户参数、过滤规则、设定应用于从电子邮件服务器得到电子邮件消息。
  - 1) 应用事件和消息过滤规则——基于头信息和收信人的地址。(例如：漫游)
  - 2) 内容屏蔽——基于防止垃圾邮件和病毒的信息
  - 3) 应用以下过滤器的机制：
    - 阅读过滤规则；
    - 通知过滤器；
    - 事件过滤器。
- c) 当收到请求的时候像用户发送事件。
- d) 允许用户顺序地或同时地使用多个移动电子邮件客户端。
- e) 对每一个定义的消息，支持定义、激活或者结束对它的自动回复。  
在自动回复功能中避免任何的邮件回路。
- f) 对扩展的邮件服务的支持：
  - 1) 在没有下载的情况下转发-基于编辑过的消息部分, 额外的或附加的内容重组一个新的电子邮件消息。
  - 2) 在没有下载的情况下回复-基于编辑过的消息部分, 额外的或附加的内容重组一个新的电子邮件消息。
  - 3) 估计下载事件——在下载邮件及其附件前评估下载消息内容的时间。
  - 4) 内容改写。
- g) 为每一个消息和事件识别源电子邮件 服务器和账户，这样使得客户端能够根据源处理消息和事件。例如：为不同的账户设置不同的文件夹和不同的图标。
- h) 为统一的测量机制收集测量信息。
- i) 通知移动电子邮件客户端任何处理错误。

#### 6.1.4.5 事件处理



电子邮件事件可以起始于电子邮件服务器或移动电子邮件客户端。只有当移动电子邮件客户端在线的时候，移动电子邮件服务器才能从移动电子邮件客户端收到电子邮件事件。类似的：只有当电子邮件服务器在线的时候，移动电子邮件服务器才能从电子邮件服务器收到电子邮件事件。

一般来说，每一个电子邮件事件都是反射给对方的：起始于客户端的电子邮件事件到电子邮件服务器，起始于服务器的电子邮件事件到电子邮件客户端，然而，起始于服务器的电子邮件事件要遵守过滤规则。

移动电子邮件服务器使用带内和带外通知将电子邮件事件传递到移动电子邮件客户端。

#### 6.1.4.6 媒体转换

有时，移动电子邮件客户端可能遇到这样的附件：在下载以前可以进行转化。移动电子邮件客户端这样做，可能是因为功能（内存，缺少编解码器，显示尺寸）所限，它不能处理这个附件。也可能是因为它想要对附件进行转化。

移动电子邮件服务器可以自己执行要求的转化，但是这种转换不在本技术报告描述范围之内。本技术报告只是列举通过移动电子邮件协议调用其它引擎的机制。

### 6.2 流

这一节描述与使用移动电子邮件引擎相关的高层的逻辑流。

#### 6.2.1 在使用移动电子邮件服务之前

在终端用户开始使用移动电子邮件服务之前，服务提供商可以采用各种操作来帮助用户使用服务——最终允许用户在没有修改任何设定的情况下使用服务。这些操作包括（但不仅仅限于）：

- a) 在移动电子邮件服务器上对用户进行基本的设定：
  - 1) 过滤规则初始化；
  - 2) 用户参数初始化；
  - 3) 邮箱设计初始化。
- b) 远程配置用户的客户端：
  - 1) 根据使用的部署模型使用移动电子邮件服务器，电子邮件服务器和代理去配置：
    - 用户名/密码；
    - 地址和端口设定。
  - 2) 带外 通知设定：
    - 可用承载；
    - 支持的载荷内容；
    - 密钥。

#### 6.2.2 使用服务

移动电子邮件业务的使用一般包括以下：

- a) 建立移动电子邮件会话；
- b) 使用移动电子邮件服务；
- c) 挂起移动电子邮件服务。

##### 6.2.2.1 建立移动电子邮件会话

为了使用移动电子邮件服务，移动电子邮件客户端需要建立移动电子邮件会话。移动电子邮件会话是使用移动电子邮件协议在移动电子邮件客户端和移动电子邮件服务器之间建立的。移动电子邮件客户端和移动电子邮件服务器之间的通信也是使用移动电子邮件协议。移动电子邮件客户端负责维护移动电子邮件会话。

移动电子邮件服务器接受移动电子邮件客户端的请求。移动电子邮件服务器需要跟合适的电子邮件服务器建立连接。移动电子邮件服务器使用电子邮件协议与电子邮件服务器进行通信。当移动电子邮件

服务器和电子邮件服务器之间的连接可用的时候,移动电子邮件服务器生成移动电子邮件客户端要求的移动电子邮件会话,并且通知移动电子邮件客户端。

#### 6.2.2.2 使用移动电子邮件服务

移动电子邮件客户端和移动电子邮件服务器之间使用建立的移动电子邮件会话交换电子邮件事件和电子邮件数据,这一般意味着一个持续的由移动电子邮件协议提供的移动电子邮件队列。然而,一般情况下,每次移动电子邮件会话只执行一次移动电子邮件队列(在建立移动电子邮件会话之后),新的电子邮件事件使用通知从移动电子邮件服务器传到移动电子邮件客户端,使用移动电子邮件协议从移动电子邮件客户端传到移动电子邮件服务器。

在联机或者离线的时候都可以使用移动电子邮件服务,唯一的不同是:当移动电子邮件客户端离线的时候,新的事件不能反映到对方,除非这些事件使用带外通知被告知。

起始于客户端的电子邮件事件是在用户正在管理他的电子邮件数据的时候生成的。起始于服务器端的电子邮件事件是当移动电子邮件服务器检测到用户邮箱有所变化的时候生成的,这里的变化一般是指邮箱中的新邮件可用,然而,也可能是指同一个邮箱中的电子邮件数据正在从另一个客户端被管理。

#### 6.2.2.3 挂起移动电子邮件服务

移动电子邮件客户端会希望在脱机和在线状态之间交换,以节省空中传输的时间和通信量、电池使用寿命等等。因此,移动电子邮件客户端会在一段时间的非活动状态后挂起会话。在挂起的时间段内,到移动电子邮件服务器的连接会中断。当移动电子邮件客户端检测到激活(可能是本地的电子邮件事件请求连接或者是重要的远程电子邮件事件被通知)以后,它就会重新建立到移动电子邮件服务器的连接并且执行移动电子邮件队列来得到一个邮箱的最新的视图。

最终,当用户很可能对电子邮件没有任何兴趣的时候,移动电子邮件客户端会在不挂起会话的情况下断开连接。

### 7 移动电子邮件传输协议

移动电子邮件传输协议可采用IETF Lemonade(包括一系列标准)(参见附录A),OMA DS等。

## 附 录 A (资料性附录)

### 支持多样服务环境的因特网电子邮件 (Lemonade)

本附录参考IETF Lemonade工作组系列标准中的IETF RFC4550。

#### A.1 介绍

IETF Lemonade工作组致力于提供一个因特网电子邮件用于递交、传输和提取的增强协议以促进在资源受限的平台上、或基于高等待时间、受限带宽的通信连接的操作。工作的主要目标是能够保证同现存的因特网电子邮件协议互操作，以便使传统因特网用户能够接入一个无缝的业务。

Lemonade工作组未来的工作方向为与移动设备使用电子邮件相关的问题，可能包括：

- 媒体转换；
- 传输优化；
- 服务器到客户端的通知；
- 处理防火墙和中间件；
- 压缩和其他的带宽优化；
- 过滤；
- 其它的关于移动客户端的考虑。

支持多样服务环境(Diverse Service Environments)的因特网电子邮件依赖于IMAP和邮件递交协议的扩展。允许客户端(尤其是那些在内存，带宽，处理能力或其他方面受限的)高效的使用IMAP和递交协议来访问和递交邮件。包括：无须下载和上传就能前转电子邮件的能力，优化递交的能力，在与服务器连接失败的情况下高效地重新同步的能力。

#### A.2 邮件前转 (Forward without Download)

##### A.2.1 消息发送综述

发送一个电子邮件消息包含多个步骤：建立草稿、草稿编辑、消息整合、以及消息递交。

建立草稿和草稿编辑在邮件用户代理上完成。用户常常选择在服务器上保存比较复杂的消息(通过带有\Draft标记的APPEND命令)以便以后能够被邮件用户代理调回，使编辑过程继续。

消息整合是从草稿的最终修订版本和外部资源产生出一个完整的消息的过程。在整合的时候，外部数据被找回，并被插入到消息当中。

消息递交是将整合过的消息插入到如IETF RFC 2821所规定的设施中的过程，一般使用时遵循IETF RFC 4409中的规定。

##### A.2.2 传统策略

以前，消息完全在一个消息用户代理上被初始化，编辑，整合，尽管草稿可以被保存到服务器上并且随后可以从服务器上提取。完成的文本被传到一个消息递交代理 (Message Submission Agent) 以备发送。

在编辑和整合的过程中经常没有清晰的界限。如果一个消息被转发了，它的内容也会立即被取回并且插入到消息文本中。类似的，当外部的内容被插入或者被附加的时候，这个内容也会被立即取回并成为草稿的一部分。

因而，所保存的每一份草稿和随后传输草稿的整个内容作为消息递交。



在过去，这不是什么难题，因为草稿，外部数据，以及消息整合机制是处在同一个系统上的，像邮件用户代理。最普遍的问题就是超过了磁盘的容量。

### A. 2. 3 分步描述

模型1区分了邮件用户代理(MUA), IMAP4Rev1服务器, 和SMTP递交服务器, 如图A. 1所示:

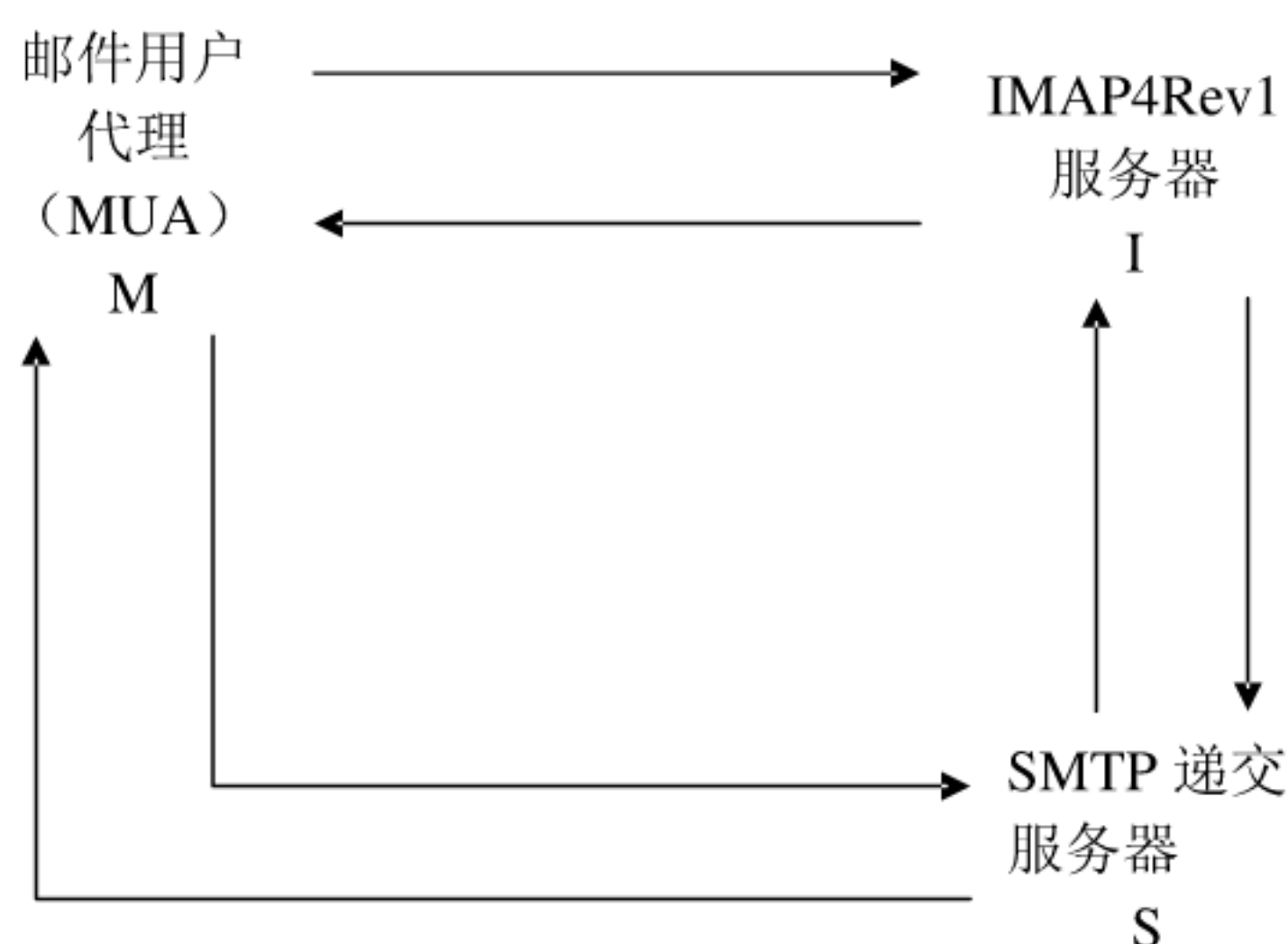


图 A. 1 支持多样服务环境的因特网电子邮件所规定的前转

电子邮件可能包含处于IMAP服务器上的数据分片，支持多样服务环境的因特网电子邮件所规定的前转允许邮件用户代理编辑并转发这类电子邮件而不需要将这些数据分片事先下载到客户端。

根据消息整合发生的地点，有两种进行前转的方法：第一种方案如IETF RFC 4469所描述，使用扩展的APPEND命令在消息存储器编辑草稿，并在IMAP服务器上发起消息的整合。第二种方案如IETF RFC 4468所描述，使用一系列的BURL和BDAT命令递交和整合消息数据，这里的数据来自客户端和外部的数据（通过提供的URL得到）。下面的两节对如何达到前转提供分步的介绍。

#### A. 2. 3. 1 使用IMAP CATENATE扩展的消息整合

在Lemonade的前转策略如IETF RFC 4468或IETF RFC 4469所描述的方案中，邮件用户代理首先对消息编辑和排版。然后使用如IETF RFC 4469所描述，扩展在IMAP服务器上创建消息——即通过传输新的文本和对它们进行整合来创建消息。客户端用如IETF RFC 4315所描述的IMAP扩展获得所创建消息的UID(Unique Identifier)。最后，给定一种如IETF RFC 4467所描述格式的URL到如IETF RFC 4409所描述的服务器，以使用如IETF RFC 4468所描述的扩展进行递交。

支持这个用例的相关流程包括（以下“M”，“I”，“S”分别代表由“客户端的消息用户代理（messaging user agent）”，“IMAP e-mail服务器”和“SMTP递交服务器”发出的命令行。下同）：

M: {到I} 客户端连接到IMAP server, 可选的开启TLS(如果要求数据保密)，鉴权，打开邮箱(下面例子中的“INBOX”)并且获得消息体结构。

例子：

```

M: A0051 UID FETCH 25627 (UID BODYSTRUCTURE)
I: * 161 FETCH (UID 25627 BODYSTRUCTURE (("TEXT" "PLAIN"
("CHARSET" "US-ASCII") NIL NIL "7BIT" 1152 23) (
"TEXT" "PLAIN" ("CHARSET" "US-ASCII" "NAME"
"trip.txt")
"<960723163407.20117h@washington.example.com>")
  
```

"Your trip details" "BASE64" 4554 73) "MIXED"))

I: A0051 OK completed

M: {到I} 客户端调用CATENATE——它允许邮件用户代理在IMAP服务器上使用新的数据连同若干已经存在于IMAP服务器上的消息部分相结合来创建消息。

注意这一步的例子没有使用LITERAL+扩展。没有LITERAL+, 新消息要使用三次往返传输才能构建, 如果使用了LITERAL+, 只需要一次往返传输。

M: A0052 APPEND Sent FLAGS (\Seen \$MDNSent)

CATENATE (TEXT {475})

I: + Ready for literal data

M: Message-ID: <419399E1.6000505@caernarfon.example.org>

M: Date: Thu, 12 Nov 2004 16:57:05 +0000

M: From: Bob Ar <bar@example.org>

M: MIME-Version: 1.0

M: To: foo@example.net

M: Subject: About our holiday trip

M: Content-Type: multipart/mixed;

M:     boundary="-----030308070208000400050907"

M:

M: -----030308070208000400050907

M: Content-Type: text/plain; format=flowed

M:

M: Our travel agent has sent the updated schedule.

M:

M: Cheers,

M: Bob

M: -----030308070208000400050907

M: URL "/INBOX;UIDVALIDITY=385759045/;

UID=25627/;Section=2.MIME" URL "/INBOX;

UIDVALIDITY=385759045/;UID=25627/;Section=2" TEXT {44}

I: + Ready for literal data

M:

M: -----030308070208000400050907--

M: )

I: A0052 OK [APPENDUID 387899045 45] CATENATE Completed

M: {到 I} 客户端使用GENURLAUTH命令来请求一个URLAUTH URL;

I: {到 M} IMAP服务器返回一个适合于稍后用URLFETCH取回的URLAUTH。

M: A0054 GENURLAUTH "imap://bob.ar@example.org/Sent;

UIDVALIDITY=387899045/;uid=45;expire=2005-10-

28T23:59:59Z;urlauth=submit+bob.ar" INTERNAL

I: \* GENURLAUTH "imap://bob.ar@example.org/Sent;

UIDVALIDITY=387899045/;uid=45;expire=

2005-10-28T23:59:59Z;urlauth=submit+bob.ar:

```
internal:91354a473744909de610943775f92038"
```

```
I: A0054 OK GENURLAUTH completed
```

M: {到 S} 客户端连接到邮件递交服务器开始一个新的邮件传输。它使用BURL让SMTP递交服务器从IMAP服务器获取消息内容。这允许邮件用户代理授权SMTP递交服务器访问作为CATENATE步结果的消息组成。注意在一个成功的STARTTLS命令以后，第二个EHLO命令是必须的。而且应该注意到，如果第二个EHLO答复没有列出任何的BURL选项，可能会有第三个EHLO请求。

```
S: 220 owlry.example.org ESMTP
M: EHLO potter.example.org
S: 250-owlry.example.com
S: 250-8BITMIME
S: 250-BINARYMIME
S: 250-PIPELINING
S: 250-BURL imap
S: 250-CHUNKING
S: 250-AUTH PLAIN
S: 250-DSN
S: 250-SIZE 10240000
S: 250-STARTTLS
S: 250 ENHANCEDSTATUSCODES
M: STARTTLS
S: 220 Ready to start TLS
...TLS negotiation, subsequent data is encrypted...
M: EHLO potter.example.org
S: 250-owlry.example.com
S: 250-8BITMIME
S: 250-BINARYMIME
S: 250-PIPELINING
S: 250-BURL imap
S: 250-CHUNKING
S: 250-AUTH PLAIN
S: 250-DSN
S: 250-SIZE 10240000
S: 250 ENHANCEDSTATUSCODES
M: AUTH PLAIN aGFycnkAaGFycnkAYWNjaW8=
S: 235 2.7.0 PLAIN authentication successful.
M: MAIL FROM:<bob.ar@example.org>
S: 250 2.5.0 Address Ok.
M: RCPT TO:<foo@example.net>
S: 250 2.1.5 foo@example.net OK.
M: BURL imap://bob.ar@example.org/Sent;UIDVALIDITY=387899045/;
uid=45/;urlauth=submit+bar:internal:
91354a473744909de610943775f92038 LAST
```



.....

S: {to I} mail submission server使用URLFETCH得到被发出的消息。

I: {to S} 提供作为CATENATE步构造结果的消息

邮件递交服务器打开到IMAP服务器的IMAP连接。

```
I: * OK [CAPABILITY IMAP4REV1 STARTTLS NAMESPACE LITERAL+
    CATENATE URLAUTH UIDPLUS CONDSTORE IDLE] imap.example.com
    IMAP server ready
S: a000 STARTTLS
I: a000 Start TLS negotiation now
...TLS negotiation, if successful - subsequent data
    is encrypted...
S: a001 LOGIN submitserver secret
I: a001 OK submitserver logged in
S: a002 URLFETCH "imap://bob.ar@example.org/Sent;
    UIDVALIDITY=387899045/;uid=45/;urlauth=submit+bob.ar:
    internal:91354a473744909de610943775f92038"
I: * URLFETCH "imap://bob.ar@example.org/Sent;
    UIDVALIDITY=387899045/;uid=45/;urlauth=submit+bob.ar:
    internal:91354a473744909de610943775f92038" {15065}
...message body follows...
S: a002 OK URLFETCH completed
I: a003 LOGOUT
S: * BYE See you later
S: a003 OK Logout successful
```

注意如果IMAP server在greeting中没有发送CAPABILITY回复代码的话，邮件递交服务器必须发送CAPABILITY 命令来了解支持的IMAP扩展--如IETF RFC 3501所描述。

而且，如果没有要求数据加密，邮件递交服务器在发送LOGIN命令之前可以省略STARTTLS命令

S: {到 M} 递交服务器整合全部的信息，如果整合成功，它向邮件用户代理回复OK。

```
S: 250 2.5.0 Ok.
```

M: {到 I} 客户端在IMAP服务器上标记包含转发的附件的消息。

```
M: A0053 UID STORE 25627 +FLAGS.SILENT ($Forwarded)
I: * 215 FETCH (UID 25627 MODSEQ (12121231000))
I: A0053 OK STORE completed
```

注意：上面显示的UID STORE命令只有标记的消息在当前选中的邮箱的时候才起作用；否则的话，它请求一个SELECT。这个命令可以被省略。没有被标记的FETCH 回复应归于如IETF RFC 4551的描述。

#### A. 2. 3. 2 使用SMTP CHUNKING和BURL 扩展的消息整合

在如IETF RFC 4468/IETF RFC 3030所描述的Lemonade前转机制中，消息最初在邮件用户代理中被编辑和排版。在递交过程中，使用BURL和BDAT命令来生成来自多个部分的消息。新的消息体部分使用BDAT命令提供，而已经存在的消息体部分使用BURL命令中如IETF RFC 4467所描述的格式的URL引用。

支持这个用例的相关流程包括（以下“M”，“I”，“S”分别代表由“客户端的消息用户代理（messaging user agent）”，“IMAP e-mail服务器”和“SMTP递交服务器”发出的命令行。下同）：

M: {到 I } 客户端连接到IMAP server, 可选的开启TLS(如果要求数据保密), 鉴权, 打开邮箱(下面例子中的"INBOX")并且获得消息体结构。

例子:

```
M: A0051 UID FETCH 25627 (UID BODYSTRUCTURE)
I: * 161 FETCH (UID 25627 BODYSTRUCTURE (("TEXT" "PLAIN"
("CHARSET" "US-ASCII") NIL NIL "7BIT" 1152 23) (
"TEXT" "PLAIN" ("CHARSET" "US-ASCII" "NAME"
"trip.txt")
"<960723163407.20117h@washington.example.com>"
"Your trip details" "BASE64" 4554 73) "MIXED"))
I: A0051 OK completed
```

M: {到 I} 客户端使用GENURLAUTH命令请求URLAUTH URL(如IETF RFC 4467的描述), 它是将要被整合的消息片的引用。

I: {到 M} IMAP服务器返回适合于稍后用URLFETCH取回的URLAUTH URL。

```
M: A0054 GENURLAUTH "imap://bob.ar@example.org/INBOX;
UIDVALIDITY=385759045/;UID=25627/;Section=2. MIME;
expire=2006-10-28T23:59:59Z;urlauth=submit+bob.ar"
INTERNAL "imap://bob.ar@example.org/INBOX;
UIDVALIDITY=385759045/;UID=25627/;Section=2;
expire=2006-10-28T23:59:59Z;urlauth=submit+bob.ar" INTERNAL
I: * GENURLAUTH "imap://bob.ar@example.org/INBOX;
UIDVALIDITY=385759045/;UID=25627/;Section=2. MIME;
expire=2006-10-28T23:59:59Z;urlauth=submit+bob.ar:
internal:A0DEAD473744909de610943775f9BEEF"
"imap://bob.ar@example.org/INBOX;
UIDVALIDITY=385759045/;UID=25627/;Section=2;
expire=2006-10-28T23:59:59Z;urlauth=submit+bob.ar:
internal:BEEFA0DEAD473744909de610943775f9"
I: A0054 OK GENURLAUTH completed
```

M: {到 S} 客户端连接到邮件递交服务器开始一个新的邮件传输。它使用BURL让SMTP递交服务器从IMAP服务器获取将要发送的消息片。注意在一个成功的STARTTLS命令以后, 第二个EHLO命令必须的。而且应该注意到, 当且仅当第二个EHLO答复没有列出任何的BURL选项, 会有第三个EHLO请求。

```
S: 220 owlry.example.org ESMTP
M: EHLO potter.example.org
S: 250-owlry.example.com
S: 250-8BITMIME
S: 250-BINARYMIME
S: 250-PIPELINING
S: 250-BURL
S: 250-CHUNKING
S: 250-AUTH DIGEST-MD5
S: 250-DSN
```

S: 250-SIZE 10240000  
 S: 250-STARTTLS  
 S: 250 ENHANCEDSTATUSCODES  
 M: STARTTLS  
 S: 220 Ready to start TLS  
 ...TLS negotiation, subsequent data is encrypted...  
 M: EHLO potter.example.org  
 S: 250-owlry.example.com  
 S: 250-8BITMIME  
 S: 250-BINARYMIME  
 S: 250-PIPELINING  
 S: 250-BURL  
 S: 250-CHUNKING  
 S: 250-AUTH DIGEST-MD5 CRAM-MD5 PLAIN EXTERNAL  
 S: 250-DSN  
 S: 250-SIZE 10240000  
 S: 250 ENHANCEDSTATUSCODES  
 M: AUTH PLAIN aGFycnkAaGFycnkAYWNjaW8=  
 S: 235 2.7.0 PLAIN authentication successful.  
 M: EHLO potter.example.org  
 S: 250-owlry.example.com  
 S: 250-8BITMIME  
 S: 250-BINARYMIME  
 S: 250-PIPELINING  
 S: 250-BURL imap imap://imap.example.org  
 S: 250-CHUNKING  
 S: 250-AUTH DIGEST-MD5 CRAM-MD5 PLAIN EXTERNAL  
 S: 250-DSN  
 S: 250-SIZE 10240000  
 S: 250 ENHANCEDSTATUSCODES  
 M: MAIL FROM:<bob.ar@example.org> BODY=BINARY  
 S: 250 2.5.0 Address Ok.  
 M: RCPT TO:<foo@example.net>  
 S: 250 2.1.5 foo@example.net OK.  
 M: BDAT 475  
 M: Message-ID: <419399E1.6000505@caernarfon.example.org>  
 M: Date: Thu, 12 Nov 2004 16:57:05 +0000  
 M: From: Bob Ar <bar@example.org>  
 M: MIME-Version: 1.0  
 M: To: foo@example.net  
 M: Subject: About our holiday trip  
 M: Content-Type: multipart/mixed;

```

M:      boundary="-----030308070208000400050907"
M:
M: -----030308070208000400050907
M: Content-Type: text/plain; format=flowed
M:
M: Our travel agent has sent the updated schedule.
M:
M: Cheers,
M: Bob
M: -----030308070208000400050907
S: 250 2.5.0 OK
M: BURL imap://bob.ar@example.org/INBOX;
  UIDVALIDITY=385759045/;UID=25627/;Section=2.MIME;
  expire=2006-10-28T23:59:59Z;urlauth=submit+bob.ar:
  internal:A0DEAD473744909de610943775f9BEEF
S: 250 2.5.0 OK
M: BURL imap://bob.ar@example.org/INBOX;
  UIDVALIDITY=385759045/;UID=25627/;Section=2;
  expire=2006-10-28T23:59:59Z;urlauth=submit+bob.ar:
  internal:BEEFA0DEAD473744909de610943775f9
S: 250 2.5.0 OK
M: BDAT 44 LAST
M:
M: -----030308070208000400050907--

```

s: {到 I} 邮件递交服务器使用URLFETCH得到被发出的消息片。这个所谓的当票（“pawn-ticket”）鉴权机制，使用包含其自身鉴权凭证的URI。

I: {到 S} 返回请求的消息体部分。

邮件递交服务器打开对IMAP服务器的IMAP连接：

```

I: * OK [CAPABILITY IMAP4REV1 STARTTLS NAMESPACE LITERAL+
  CATENATE URLAUTH UIDPLUS CONDSTORE IDLE] imap.example.com
  IMAP server ready
S: a001 LOGIN submitserver secret
I: a001 OK submitserver logged in
S: a002 URLFETCH "imap://bob.ar@example.org/INBOX;
  UIDVALIDITY=385759045/;UID=25627/;Section=2.MIME;
  expire=2006-10-28T23:59:59Z;urlauth=submit+bob.ar:
  internal:A0DEAD473744909de610943775f9BEEF" "imap://
  bob.ar@example.org/INBOX;
  UIDVALIDITY=385759045/;UID=25627/;Section=2;
  expire=2006-10-28T23:59:59Z;urlauth=submit+bob.ar:
  internal:BEEFA0DEAD473744909de610943775f9"
I: * URLFETCH "imap://bob.ar@example.org/INBOX;

```



```

UIDVALIDITY=385759045/;UID=25627/;Section=2.MIME;
expire=2006-10-28T23:59:59Z;urlauth=submit+bob.ar:
internal:A0DEAD473744909de610943775f9BEEF" {84}
...message section follows...
"imap://bob.ar@example.org/INBOX;
UIDVALIDITY=385759045/;UID=25627/;Section=2;
expire=2006-10-28T23:59:59Z;urlauth=submit+bob.ar:
internal:BEEFA0DEAD473744909de610943775f9" {15065}
...message section follows...
S: a002 OK URLFETCH completed
I: a003 LOGOUT
S: * BYE See you later
S: a003 OK Logout successful

```

注意如果IMAP服务器在greeting中没有发送CAPABILITY回复代码的话，邮件递交服务器必须发送CAPABILITY命令来了解支持的IMAP扩展——如IETF RFC 3501所描述。

而且，如果要求数据加密，邮件递交服务器在发送LOGIN命令之前应该开启STARTTLS命令

S: {to M} 递交服务器整合全部的信息，如果整合成功，它通过向上一个BDAT命令发送250回复通知消息的接收方。

```
S: 250 2.5.0 Ok, message accepted.
```

M: {to I} 客户端在IMAP服务器上标记包含转发的附件的消息。

```

M: A0053 UID STORE 25627 +FLAGS.SILENT ($Forwarded)
I: * 215 FETCH (UID 25627 MODSEQ (12121231000))
I: A0053 OK STORE completed

```

注意：上面显示的UID STORE命令只有标记的消息在当前选中的邮箱的时候才起作用；否则的话，它请求一个SELECT. 这个命令可以被省略。没有被标记的FETCH 回复应归于如IETF RFC 4551的描述。

#### A. 2. 4 当票 (pawn-tickets) 机制的安全考虑

所谓的当票 (pawn-ticket) 授权机制使用这样一个URI, 它使用如IETF RFC 4467所描述，包含了它自己的授权证书。这种机制的优点是：如果没有客户端生成的当票 (pawn-ticket), SMTP 递交如IETF RFC 4409所描述，服务器不能访问如IETF RFC 3501所描述服务器上的任何数据。

当票 (pawn-ticket) 只授权访问那些，SMTP递交服务器被授权访问的特定的数据，可以被客户端取消授权，其权利也有时间有效性限制。

#### A. 2. 5 文件副本拷贝 (file carbon copy) 问题

文件副本拷贝 (fcc) 问题是指将一个消息的副本传送到一个文件副本拷贝接收者。迄今为止，关于文件副本拷贝最通常的例子是：对于已发出去的邮件，客户端在“发件箱”或“已发送”邮件箱中保留一份副本。

依惯有策略，在一个独立的步骤中，邮件用户代理将消息写入文件副本拷贝目标文件，这样可以有效的减少传输到消息递交代理的副本。这个步骤可以是写到一个本地磁盘文件或者APPEND到IMAP服务器上的邮件箱。后者是“反复网络数据传输”中的一种，这正是文件副本拷贝问题所表现出来的一个问题。

如IETF RFC 4469所描述的扩展可以用来解决文件副本拷贝问题。为所外发的邮件，特意在邮件箱中构造最后咨文。注意，如IETF RFC 4469所描述的扩展只能在服务器发起用于递交的出局消息时才能创建一条单独的消息。该条消息的其它拷贝，可以在同一服务器上，使用一或多条COPY命令创建。

#### A. 2. 6 \$Forwarded IMAP关键字注册

多个IMAP客户端使用\$Forwarded IMAP 关键字以指定该条消息内嵌到一条新消息或作为新消息的附件重发到另一个电子邮件地址。一个邮件客户端在它成功的将消息转发到另一个电子邮件地址的时候将这个关键字置位。这个关键字的典型用法是为一个已经转发的消息显示一个不同的(或者附加的)标记。一旦设定,这个标记不能被清除。

服务器必须能够保存\$Forwarded关键字。它们必须在COPY操作时维护它。服务器必须支持 SEARCH 关键字\$Forwarded。

### A.3 消息递交

邮件递交服务器应该实现以下的SMTP扩展以使得消息递交高效。Lemonade客户端应该利用这些特性。

#### A.3.1 流水线操作

移动客户端通常所使用的网络具有相对较高的时延。在一个事务中避免往返传输对减少带宽使用和总的传输时间有很大的益处。由于这个原因,符合Lemonade规范的邮件递交服务器必须支持SMTP服务扩展以支持命令流水线操作(Pipelining)。

在可能的情况下客户端应该流水线SMTP命令。

#### A.3.2 支持DSN

符合Lemonade规范的邮件递交服务器必须支持SMTP服务扩展以支持传递状态通知DSN(Delivery Status Notification)。

#### A.3.3 消息大小声明

符合Lemonade规范的邮件递交服务器必须支持SMTP服务扩展以支持消息大小声明。

符合Lemonade规范的邮件递交服务器在实施消息大小限制以前,必须展开所有的BURL部分。

符合Lemonade规范的应该使用消息大小声明。尤其,当客户端知道消息超过了递交服务器通知的最大消息,它不能向邮件递交服务器发送消息。

#### A.3.4 支持增强状态码Enhanced Status Code

符合Lemonade规范的邮件递交服务器必须支持SMTP服务扩展以返回增强错误码。

#### A.3.5 传输层安全TLS (Transport Layer Security)

符合Lemonade规范的邮件递交服务器必须支持SMTP服务扩展以保护SMTP over TLS,如IETF RFC 3207所描述。

### A.4 快同步

符合Lemonade规范的IMAP服务器必须支持CONDSTORE (如IETF RFC 4551所描述)扩展。它通过让服务器返回所有的自从上次邮箱同步标记后的标签改变允许客户端快速的同步任何邮箱。

如IETF RFC 4549所描述的显示如何进行快速的邮箱同步。

### A.5 附加的IMAP扩展

符合Lemonade规范的IMAP服务器必须支持NAMESPACE (如IETF RFC 2342所描述)扩展。这种扩展允许客户端发现共享的邮箱和属于其他用户的邮箱。

符合Lemonade规范的必须支持LITERAL+ (如IETF RFC 2088所描述)扩展。该扩展允许客户端每当发送非同步文字时,节省往返传输

符合Lemonade规范的IMAP服务器必须支持IDLE (如IETF RFC 2177所描述)扩展。这个扩展允许客户端收到关于在所选邮箱中发生的变化的即时通知。

符合Lemonade规范的IMAP服务器必须支持IMAP over TLS,如IETF RFC 3501所要求的。



## A.6 安全性考虑

### A.6.1 递交的消息的加密保护

当客户端递交新的消息的时候，链路保护，比如TLS，防范偷听者获取递交的消息内容。这是一种相当有价值的计算方法。但是，只要使用BURL关联文本而不是将文本直接提交，即使不使用TLS，也不会有更大的风险。如果没有使用BURL，偷听者能够访问消息的全部内容。如果使用了BURL，偷听者可能会也可能不会得到这样的访问，这取决于使用的BURL的形式。例如，有些形式限制只有被授权的实体(作为递交服务器或者特定的用户)才能使用URL。

### A.6.2 传输层安全TLS (Transport Layer Security)

当Lemonade客户端使用BURL扩展进行邮件递交的时候，要求向邮件递交服务器发送一个URLAUTH权标，这种权标应当被保护不被侦听，以防可能会把消息内容泄漏给攻击者的重放攻击。基于TLS的对邮件递交路径的加密将针对这种攻击提供保护。

Lemonade客户端在使用基于BURL的消息递交时，应当使用受TLS保护的IMAP和邮件递交通道来防止URLAUTH被窃听。

符合Lemonade规范的邮件递交服务器在使用Lemonade客户端提供的URLAUTH权标取回消息内容时应当使用受TLS保护的IMAP连接。

当一个客户端使用SMTP STARTTLS 发送一个涉及非公开信息的BURL命令的时候，用户会希望整个消息内容将被秘密的处理。为了达到这种预期，当获取URL引用的数据的时候，消息递交服务器应该使用STARTTLS或者一种能提供等效的数据加密的机制。

### 参考文献

- [1]. OMA 移动电子邮件需求文档 OMA-RD-Mobile\_Email-V1\_0-20051018-C
- [2]. OMA 移动电子邮件架构文档 OMA-AD-Mobile\_Email -V1\_0\_0-20070308-D
- [3]. OMA 移动电子邮件技术规范 OMA-TS-Mobile\_Email -V1\_0-20070110-D
- [4]. IETF RFC 4416(支持多样服务环境的因特网消息的目标 Goals for Internet Messaging to Support Diverse Service Environments )
- [5]. IETF RFC 4550(支持多样服务环境的因特网电子邮件描述 Internet Email to Support Diverse Service Environments (Lemonade) Profile)