Executive Overview........................................................................................................ 2
Mobile Push Mail Market Opportunity........................................................................ 2
Standards-Based Approach To Mobile Push Mail ..................................................... 3
Oracle’s Vision............................................................................................................. 3
Key Highlights of Mobile Push Mail: ................................................................. 3
Standardization Overview.......................................................................................... 5
P-IMAP Protocol........................................................................................................ 5
Mobile Push Mail Protocol Comparison.............................................................. 6
P-IMAP Components and Architecture................................................................. 7
P-IMAP Gateway....................................................................................................... 7
P-IMAP Client .......................................................................................................... 7
Mobile Connectors................................................................................................. 8
Mobile Enablers....................................................................................................... 8
Mobile Push Mail Experience.................................................................................. 8
P-IMAP Deployment Scenarios.................................................................................. 9
Hosted Email Service:............................................................................................ 9
Push Enabled Email Server:.................................................................................. 9
Hosted Push Enabled Email:.................................................................................. 9
P-IMAP Specifications Status at IETF and OMA..................................................... 10
Security Considerations............................................................................................ 11
Security In Design................................................................................................. 11
Security During Deployment.................................................................................. 11
Security During Operations.................................................................................... 12
Benefits to Value Chain Players............................................................................... 12
Enterprises.............................................................................................................. 12
Mobile Operators and Service Providers............................................................ 12
Device and Terminal Manufactures......................................................................... 13
Developers and ISVs.............................................................................................. 13
End Users................................................................................................................ 13
Conclusion.............................................................................................................. 13
Glossary of Terms..................................................................................................... 15
EXECUTIVE OVERVIEW

Mobile and wireless technologies have made great progress over the last decade, with devices, networks, supporting IT infrastructure, and applications approaching the level of power, performance, and stability that enterprises need to become mobile. Collaboration, Messaging and Email applications are among the first key enterprise applications that will be mobilized. However, widespread full-scale enterprise deployments of such applications remain low.

This low market adoption rate of mobile applications is largely due to some key challenges encountered by enterprises today, such as:

- Inter-operability (device-to-device)
- Inter-connectivity (network-to-network)
- Inter-working (application-to-device-to-network)
- End-to-end security (between the mobile client and server/proxy)
- Total cost of ownership

Moreover, the user experience of mobile access to applications today varies based on the type of mobile devices, the mobile network operators and the back-end server capabilities and most of the current commercially available mobile applications are proprietary.

Mobile email is one of the most important mobile enterprise applications today. Various terminologies such as “mobile email”, “wireless email”, “push email”, etc., have been used to refer to accessing email via mobile devices. In this white paper, we use the term “Mobile Push Mail” to refer to the technology that provides the most preferred user experience. This white paper focuses on the ‘mobile push mail’ market opportunities and the key obstacles hindering the growth of this market. It then discusses how a standards-based approach to providing the underlying technologies can accelerate the mobile push mail market growth, by providing a consistent user experience using any mobile device over any mobile network and any email server, while lowering the total cost of delivering such a solution to the enterprises. Since the industry standards for mobile push mail applications are not established yet, Oracle and key strategic partners are leading the efforts for the standardization of mobile push mail based on open P-IMAP specifications, through active participation in global standards organizations such as IETF and OMA.

This white paper is written for Enterprise IT professionals, Mobile Device and Terminal Manufacturers, Mobile Network Operators and Service Provider, and Developers and Independent Software Vendors interested in understanding the Oracle’s vision and the corresponding technologies for mobile push mail solutions.
MOBILE PUSH MAIL MARKET OPPORTUNITY

The total number of mobile network subscribers globally has already surpassed one billion, but according to Gartner [www.gartner.com], only a very small percentage of all workers have mobile access to their emails. Ovum [www.ovum.com] estimates that there are about 3-4 million mobile email users today, and growing rapidly. Enterprises are in the early phases of the mobile email adoption, with no more than a few million users globally, but analysts predict substantial mobile email uptake, as Mobile Operators offering more and more point solutions globally. However, it is difficult to estimate the total size of the addressable mobile push mail market: it ranges anywhere from a few key executives in enterprises to all mobile workers in all industries, including those who have never used email before.

The current mobile push mail vendors offer proprietary solutions with support for specific email servers and for a limited set of mobile devices. As Mobile Operators and Service Providers look to offer a broader set of valuable mobile services to their enterprise customers, they are looking to expand their mobile push mail offerings to multi-vendor, standards-based solutions with support and optimization for a plethora of mobile channels, devices, and email servers working seamlessly across various networks.

End-to-end security, device costs, network usage costs and difficulty in proving the ROI case are among the key concerns most frequently cited by enterprises as barriers to mobile push mail adoption. Although the ROI for mobile push mail solutions was not a significant barrier for early adopters, who deployed solutions for a small number of key executives, as solutions become mainstream, enterprises are starting to demand quantifiable ROI on solutions that are used by all.

Enterprises’ interest in mobile email is almost entirely concentrated on mobile push mail applications, where email is literally ‘pushed’ in real-time to mobile devices, without any action necessary from the email recipients, thus providing the best user experience. Interest among Mobile Operators and Service Providers, Device and Terminal Manufacturers, Independent Software Vendors or customers in services that do not offer or do not have plans to offer some form of mobile push mail capabilities is decreasing.

The best known mobile push mail provider, is the Research In Motion (RIM)®, whose purpose-built handheld, BlackBerry®, is considered the ‘benchmark device’ for mobile email. RIM’s BlackBerry is the leading dedicated, end-to-end solution for mobile push email. However majority of enterprise deployments of RIM BlackBerry are small with an average of 10-20 users per site, and although RIM’s market share is strong now, most of the mobile push mail market has yet to be won by anyone.
STANDARDS-BASED APPROACH TO MOBILE PUSH MAIL

Open standards enabling mobile services interoperability are critical to maturity and stability of the mobile market growth, in general. Without open standards, enterprises will not undertake mobilizing their organizations in a meaningful way.

Today, OMA’s Data Sync [formerly SyncML] offers a suitable foundation to support an open standards-based push PIM solution. The same is not true for mobile [push-based] email, where only proprietary solutions exist today. RIM’s BlackBerry solution is based on the proprietary BlackBerry Enterprise Server [BES] that requires the Mobile Operators to use RIM’s proprietary Network Operation Center (NOC), exclusive to RIM devices. Microsoft® solution is limited to Microsoft smart devices and Microsoft Exchange® Servers. Niche vendors such as Good Technology, Visto, and others offer closed end-to-end solutions with proprietary client and server components.

A standards-based solution will benefit all, by allowing all the players in the value chain to interoperate with each other to provide more efficient solutions than today’s proprietary deployments at a lower total cost of ownership – while allowing for support at feature parity across any device, any network, or any email server. This will free Mobile Operators and Service Providers from deploying expensive and proprietary solutions with risky long-term futures.

ORACLE’S VISION

Oracle’s Mobile Push Mail, a component of the Oracle® Collaboration Suite, is based on open industry standards and specifications. Oracle’s Mobile Push Mail solution relies on IETF’s P-IMAP specifications, as well as relying on other open standards such as OMA’s Data Sync, OMA client provisioning and device management. Oracle Collaboration Suite offers a complete open standards-based end-to-end secure solution for Mobile Push Mail and PIM.

Key Highlights of Mobile Push Mail:

Real-time, Always-on Push: P-IMAP-based mobile push mail solution provides end-to-end secure, behind-the-firewall server solution to real-time mobile push mail to all mobile devices, in particular always-on (as well as other) devices. Mobile push mail solutions push email to mobile devices in real time without requiring any user intervention.

Cradle-free, Continuous, Two-way Sync: Continuous, two-way real-time solution ensures that any changes on the mobile device (i.e. delete an email, respond to an email, read to unread) are wirelessly synchronized with the email server in real-time, according to user’s preferences. Similarly, new emails as well as any other changes from the email server are wirelessly reflected on the mobile device in real-time, according to user’s preferences. No additional cradle, desktop software or manual reconciliation is required.
**In-band and Out-of-band Notification:** Mobile push mail solution uses specific network feature to send notifications in two ways:

a) In-band notification via the P-IMAP gateway through the existing P-IMAP connection;

b) Out-of-band notification via notification server, which sends the appropriate type of notification by relying on a driver architecture to find the appropriate notification engine (e.g. SMS-C) to send the notification outside the data connection: via SMS, MMS, WAP Push or within the same data connection (e.g. SIP notification or UDP notification). New notification channels could be added by adding appropriate drivers to the notification server.

**Folder and Attachment Support:** Mobile push mail solution includes full support to push any IMAP folder, and push/truncate (partial download) /open/view attachments. The attachments can be converted and adapted to the capabilities of the mobile device.

**Bandwidth Optimization:** P-IMAP optimizes the bandwidth requirements to access email by optimizing the protocols, allowing partial download of email body and attachments, compression of email message and forward without download of email with attachments.

**Filter Support:** Allows user to create/modify filters to specify which email they want to be pushed from desktop and from their mobile devices.

**Open standards-based Device & Network-agnostic Solution:** Mobile push mail solution is completely based on open standards and is truly device, transport protocol, and network-agnostic. P-IMAP solution leverages existing IMAP and TLS/HTTPS technology stack, and is completely open to be adopted by any mobile device or email server. Additionally, it is also possible for Developers and Independent Software Vendors to develop compliant client components that rely on other transport, notification schemes, and network optimization.

P-IMAP is a NOC-less (Network Operation Center) solution and an enterprise or email provider can provide mobile push mail for any mobile device for any email server, with a network agnostic push experience.

**End-to-end Secure, Reliable, Enterprise-class Solution:** Deployed behind the firewall, mobile push mail solution provides an end-to-end secure and reliable enterprise-class solution for mobile users. Mobile push mail solution provides end-to-end security (HTTPS or TLS), and allows over-the-air (OTA) policy management and client configuration.

**Graceful Degradation:** With mobile push email, it is also possible to access email via multiple channels listed below, without the optimized push email experience, if the P-IMAP client is not available:
STANDARDIZATION OVERVIEW

Industry standards for mobile email applications are not established yet. Oracle and key strategic partners are leading the efforts for the standardization of mobile push mail based on open P-IMAP specifications through active participation in global standards organizations such as Open Mobile Alliance (OMA) and Internet Engineering Task Force (IETF).

Oracle’s Mobile Push Mail and PIM solution relies on OMA and IETF specifications. In particular Oracle’s Mobile Push Mail relies on P-IMAP, an Internet draft submitted to IETF that provides an optimization of IMAP 4.0 specification to provide push email over mobile network while offering backward compatibility to IMAP 4.0. It consists of:

- Optimizations to reduce IMAP chattiness and bandwidth requirements (macros, application level compression, filtering, notifications)
- A few new instructions to support the usage model of mobile push mail
- An explicit binding to HTTP to provide a simple solution to VPN and firewalls
- Attachment conversion and manipulation
- Network independence of the specification and notification channels
- A specification of the notifications that can be used in-band within P-IMAP exchanges (HTTP, TCP), within the same data channel (SIP notifications, UDP) or as out-of-band notifications (e.g. SMS, OMA WAP push, MMS, etc.)
- Transport level and application level encryption capabilities with key management to support end-to-end security with any possible deployment model of P-IMAP.

P-IMAP Protocol

P-IMAP is a set of IMAP-like textual semantics that can be bound to different protocols such as HTTPS and TCP/TLS plus notification channel independent notifications.

A P-IMAP client receives pushed notifications from the email server as prescribed by the P-IMAP specifications and the preferences of the user. When interacting with the server-side, for example as a result of a received
notification, the interactions are specified by P-IMAP and exchanged on the selected underlying transport protocol (to which P-IMAP is bound).

**Mobile Push Mail Protocol Comparison**

The chart below provides a high level comparison of P-IMAP and various other mobile push mail protocols, courtesy of SonyEricsson®:

<table>
<thead>
<tr>
<th></th>
<th>P-IMAP</th>
<th>OMA DS</th>
<th>IMAP Idle ++</th>
<th>OMA Email Notification</th>
<th>Blackberry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy set-up</td>
<td>X</td>
<td>X</td>
<td>(X)</td>
<td>(X)</td>
<td>X</td>
</tr>
<tr>
<td>Meeting requests</td>
<td>(X)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filtering/ Views/ Enhanced Search</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration with PIM sync</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Smart reply &amp; forwarding</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachment conversions</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Native attachments</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>IP Push</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>SMS Push</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Event-based difference sync</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compression of data</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault tolerant in networks/ firewall</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Operation-friendly Architecture</td>
<td>X</td>
<td>(X)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Enterprise-friendly architecture</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-to-end security</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Corporate Email</td>
<td>X</td>
<td>X</td>
<td>(X)</td>
<td>(X)</td>
<td>X</td>
</tr>
<tr>
<td>Consumer Email</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>(X)</td>
</tr>
</tbody>
</table>

*Figure 1- Comparison of Various Open and Proprietary Mobile Push Mail Protocols*
P-IMAP COMPONENTS AND ARCHITECTURE

Mobile push mail environment has four key components: P-IMAP Gateway, P-IMAP Clients and Mobile Enablers and Mail Connectors, as illustrated in the logical diagram below.

Since the above diagram is a logical diagram, some of the components might not be included or might be combined in actual field deployments. For example, firewalls may or may not be present in actual deployments.

P-IMAP Gateway

The P-IMAP gateway enables push email on the server side by:

- Notifying P-IMAP clients with in-band or out-of-band notifications when needed as prescribed by P-IMAP and the settings (administrator and user)
- Securely interacting with P-IMAP client via the P-IMAP protocol over the appropriate transport
- Interfacing with the email server

P-IMAP Client

The P-IMAP client provides the user with the mobile push mail experience. The P-IMAP client is an email application with an email user interface. It reacts to P-IMAP notifications as prescribed by P-IMAP and the user preferences / client settings. It interfaces with the P-IMAP gateway via the P-IMAP protocol over the appropriate transport. Typically there are firewalls between the client and the P-IMAP gateway.
Mobile Connectors
The connector, when it exists, allows the P-IMAP gateway to interact, possibly through firewalls, with any email server (e.g. IMAP4.0, POP3, IBM® Lotus Domino Server, Microsoft® Exchange, GroupWise, etc.)

Mobile Enablers
The mobile enablers allow the P-IMAP gateway to notify the P-IMAP client out-of-band (outside the P-IMAP connection). They are also used to provision over the air the P-IMAP email clients and parameters and manage the mobile devices.

MOBILE PUSH MAIL EXPERIENCE
A typical user experience with mobile push mail is as follows:

First time users access the service provider's website with a new device and registers the device’s phone number.

The service provider initiates over-the-air [OTA] provisioning of client on the new device by sending an SMS with a URL. The users clicks on the URL, which triggers the download client and configuration sequence on the mobile device. Users then choose a password, and they can now access their emails, as specified by their preferences.

Then, after receiving their emails, any action on the mobile device, such as read, delete, move, etc. is securely sent to the email server, via the same data channel or another channel (e.g. SMS). The email server, in turn, is updated based on the users’ preferences and actions on the device.
Some of the additional features of Mobile Push Mail are:

- Email attachments can be converted
- Filter can decide what to sync with the client
- Filter can be set from the client
- Client can forward email without having to download attachments.

**P-IMAP DEPLOYMENT SCENARIOS**

P-IMAP-based, Oracle Mobile Push Mail, enables a wide variety of deployment models: from hosting the entire solution at Oracle, to hosting by the Mobile Operators and Mobile Service Provider to hosting by the Enterprises, to accommodate various business and revenue models.

The different components can be deployed in a same domain or across different domains and may involve several value chain players to provide mobile email.

The different deployment models briefly are:

**Hosted Email Service:**

- The P-IMAP client are in the Mobile Operator / Service Provider network or a host network where the user is allowed to roam.
- P-IMAP gateways and email servers are also within the Mobile Operator / Service Provider domain.

**Push Enabled Email Server:**

- The P-IMAP client is in the Mobile Operator / Service Provider network or in a host network where it is allowed to roam.
- The P-IMAP gateway and the email server are within an email provider domain (e.g. Enterprise, Service Provider, etc).
- Mobile enabler are exposed by the Mobile Operator / Service Provider to the P-IMAP gateway.

**Hosted Push Enabled Email:**

- The P-IMAP client is in the Mobile Operator / Service Provider network or in a host network where it is allowed to roam.
- Mobile enabler are exposed by the Mobile Operator / Service Provider to the P-IMAP gateway.
- The email server is within an email provider domain (e.g. Enterprise, Service Provider, etc.).
- The P-IMAP gateway can be within a third party domain,
The P-IMAP gateway can be within the Mobile Operator / Service Provider (mobile push mail enabled by Mobile Operator / Service Provider).

P-IMAP SPECIFICATIONS STATUS AT IETF AND OMA

The P-IMAP specifications have been submitted to IETF. The latest version can be found at the link below (this is a working draft and the draft name and revision number are subject to change as the work at IETF Lemonade progresses):


IETF Lemonade activity provides a core protocol specification based on P-IMAP, but focused on TCP/IP. The design point of this activity is transport-layer independent.

The OMA’s mobile email activity will produce an end-to-end specification with interoperability guidelines that refers to the IETF works but also recommends specific bindings and transport. The OMA activity may also specify additional interoperable profiles for particular networks or device categories.

From Oracle’s point of view, although such activities are fully in progress, they will follow the normal specification/standardization cycle.

The overall process from Oracle’s perspective is:

- IETF (Lemonade) defines the base protocol for mobile push mail over TCP/IP in a way that is transport agnostic.
- OMA defines the end-to-end specifications for mobile push mail, including interoperability suites and other transport bindings than TCP/IP (e.g. HTTP).

The relationship between P-IMAP and other protocols is as follows:

- When bound to TCP/IP (and TLS), P-IMAP is an extension of IMAP. It is expected to evolve to match the IETF Lemonade mobile profile.
- When bound to HTTP (and HTTPS), P-IMAP looks like WebDAV with IMAP semantics with mobile/push email extensions.
- When bound to other transport and notification schemes, P-IMAP looks like IMAP semantics with mobile/push email extensions on transport that are specific or optimized for a particular network.

The latter two cases should be covered by the OMA specifications, in Oracle’s view.
SECURITY CONSIDERATIONS

Security remains a significant barrier to the adoption of mobile push mail in many enterprises. Enterprise IT departments and corporate guidelines will simply prevent any mobile application or deployment that stores, even temporarily, business information on external devices, or if they cannot control or guarantee the end-to-end encryption of data exchanges in wired or wireless networks. Mobile networks are especially critical because of the inherent capability to eavesdrop on such data exchanges.

Broadly speaking, security must be addressed at three levels:

1. Security in design
2. Security during deployment
3. Security during operations

Security In Design

P-IMAP relies on the security mechanisms provided by the underlying transport layers (e.g. HTTPS and TLS) for confidentiality and integrity of the exchanged data and authentication of their source. P-IMAP provides additional key exchange and encryption mechanisms to ensure confidentiality and integrity of out-of-band notification, if used.

P-IMAP also allows encryption of the P-IMAP message payload to guarantee end-to-end confidentiality and integrity when a P-IMAP gateway is used outside the domain of the email server. P-IMAP solutions provide mechanism that can be used when mobile device are to be revoked and data on the device deleted.

Security During Deployment

When deploying P-IMAP solutions, P-IMAP client should provide:

- Encryption of the email store
- Password protection of the mobile device
- Device / client revocation mechanism

If a P-IMAP gateway is used outside the domain of the email server, it is critical to activate XENCRIPTED to encrypt the P-IMAP payload messages. When out-of-band notifications are used to carry relevant information, these notifications should also be encrypted.

Mobile push mail solution should also appropriately authenticate clients, gateways and email servers during provisioning, when exchanging encryption keys and when accepting encrypted data.
Security During Operations
Best practices for security during operations are applicable here. For example:

- Denial of service attack should be monitored. If detected, the source of attack should be filtered out.
- Losses of mobile devices should be immediately reported. The device key should be removed and access from the mobile device denied. P-IMAP command should be issued to the mobile device to delete all data on the client and over-the-air provisioning should be sent to revoke and lockdown the device. The Mobile Operator should also be contacted to revoke network access to the mobile device (e.g. SIM/USIM deactivation, …).

BENEFITS TO VALUE CHAIN PLAYERS
Open standards-based solution will benefit all the players in the mobile email value chain.

Enterprises
Some of the key benefits to the Enterprises are:

- Provide end-to-end secure mobile push mail to all the employees, without impacting any established business processes
  - Any device
  - Any network
  - Any email server
- Retain flexibility over choice of vendors and standards-based solutions
- Reduce total cost of deployment, administration and management

Mobile Operators and Service Providers
Some of the key benefits to the Mobile Operators and Service Providers offering mobile email are:

- Gain new and incremental network and device revenues
- Satisfy demand for wireless email from their enterprise customers
- Offer as many device choices as possible
- Stimulate growth in mobility for other enterprise applications
Device and Terminal Manufactures

Some of the key benefits to the Device and Terminal Manufactures are:

- Gain new and incremental device revenues
- Establish ‘Brand’ equity with Enterprise-targeted devices
- Preserve customer preferences for their devices
- Enhance user experience by adding extra value-added features

Developers and ISVs

Some of the key benefits to the ISVs are:

- New Business Opportunities, providing:
  - P-IMAP clients
  - P-IMAP gateways / connectors to email servers:
    - POP3, Domino, Exchange, GroupWise, …

End Users

The key benefit to the end-users is:

- Freedom: anytime, anywhere secure access to their corporate emails with their preferred mobile devices and preferred mobile operators.

CONCLUSION

Mobility provides access to critical business information anytime anywhere and enables mobile workers to perform more efficiently and effectively. Corporate executives who derive directly quantifiable benefit from being constantly in contact, are increasingly adopting mobile push mail and in turn are promoting the usage of mobile push mail within their organizations, since they have experienced for themselves how beneficial mobile push mail can be in terms of responsiveness and productivity.

All the players in the mobile value chain are impacted by the lack of standards for the mobile push mail:

- Mobile Operators and Service Providers are sharing significant revenue with providers of proprietary mobile push mail solutions
- Device and Terminal Manufacturers must license proprietary solutions or forfeit support for mobile push mail as an out of the box feature
- Vendors of email software other than Microsoft may not be able to achieve feature parity with solutions designed primarily for Microsoft Exchange
- Enterprises:
- Cannot provide mobile push mail with any email server
- Cannot support mobile push mail for preferred set of mobile devices
- End-users experience inefficient or limited mobile push mail features

Oracle’s vision for Mobile Push Mail offers mobile users a low-cost and consistent experience using a standards-based mobile push mail solution. Such an open standards-based mobile push mail solution, will allow all the players in the value chain to interoperate with each other to provide an open solution while lowering the total cost of ownership for both the Mobile Operators and the Enterprises.

Oracle’s vision is to provide mobile email for everyone.
## GLOSSARY OF TERMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS</td>
<td>OMA Data Synchronization</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Secure Hyper Text Transport Protocol</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IMAP 4.0</td>
<td>Internet Mail Application Protocol version 5 (rev 1)</td>
</tr>
<tr>
<td>ISV</td>
<td>Independent Software Vendor</td>
</tr>
<tr>
<td>MMS</td>
<td>Multimedia Messaging Service</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operation Center</td>
</tr>
<tr>
<td>OMA</td>
<td>Open Mobile Alliance</td>
</tr>
<tr>
<td>OTA</td>
<td>Over the Air</td>
</tr>
<tr>
<td>P-IMAP</td>
<td>Push IMAP</td>
</tr>
<tr>
<td>PIM</td>
<td>Personal Information Management</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol Version 3</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiated Protocol</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SyncML</td>
<td>Older name for OMA DS</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport layer Security</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Access Protocol</td>
</tr>
</tbody>
</table>