

# CertifiedEmail™ – a New Trustworthy Messaging Class

Status: Early Draft (as of 18 Feb 2006)

Author: Daniel T. Dreyman, Goodmail Systems, Inc.

Submitted to: W3C Security & Usability Workshop

Identifying good mail helps to shield consumers from spam, fraud and phishing. With that goal, in October 2005, AOL and Yahoo! have announced they will introduce a new class of email called CertifiedEmail.

The service was developed and will be offered by Goodmail Systems, a California-based company. Only legitimate commercial senders with good past reputation can successfully pass Goodmail's accreditation process and will be subsequently allowed to certify their messages. Every message sent through the CertifiedEmail service is embedded with a cryptographically-secure token. The tokens are signed by Goodmail and validated by participating mailbox providers so the messages can be delivered directly to recipients' inboxes (without suffering from false positives associated with spam filters).

Of particular interest for this conference: the messages are identified in the MUA (Mail User Agent, or email client software) with the CertifiedEmail symbol—a mark that indicates to the recipient that the message is from a trusted sender and can be opened with greater confidence. The mark appears as an icon in the message list view (fig. 1) and as a prominent logo in the message view (fig. 2). Please note that the icon and logo appear in non-spoofable UI areas.

The CertifiedEmail service improves the consumer email experience, addresses the needs of legitimate senders, and empowers mailbox providers with a platform that uses state of the art security measures. This premium delivery service is available to qualified businesses that rely on email to reach their customers.

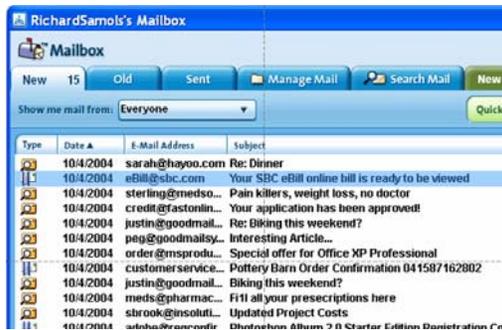


Figure 1: Message List View



Figure 2: Message View

CertifiedEmail is comprised of several components that have, to various degrees, parallels in the http transaction arena. Of particular consideration are: accreditation, presentation to the end user, end user input, real-time monitoring, the establishment of a standing reputation for senders, and the possible revocation of privileges.