

DELIVER-UPON-REQUEST SECURE ELECTRONIC MESSAGE SYSTEM

ABSTRACT

A method of delivering electronic mail messages upon requests and managing public-secret key pairs of public key cryptography in an electronic message system. A sending party sends an intend-to-deliver associated with an electronic mail message to an intended receiving party. The intended receiving party responds with a request-for-mail-content to request for the electronic mail message if the intended receiving party determines to do so. The sending party will not deliver the electronic mail message to the intended receiving party if the intended receiving party does not send the request-for-mail-content. A host computer is assigned with a unique name that is registered with authoritative organizations and can be used for establishing a connection to the host computer. The host computer provides the public keys of its account holders to the public. The initial public key of an account holder is certified by the host computer using an account password. The account holder may regenerate a public-secret key pair as often as needed. The new public key is certified by the host computer using the old public key of the account holder and becomes effective for providing to the public.

FIG. 1