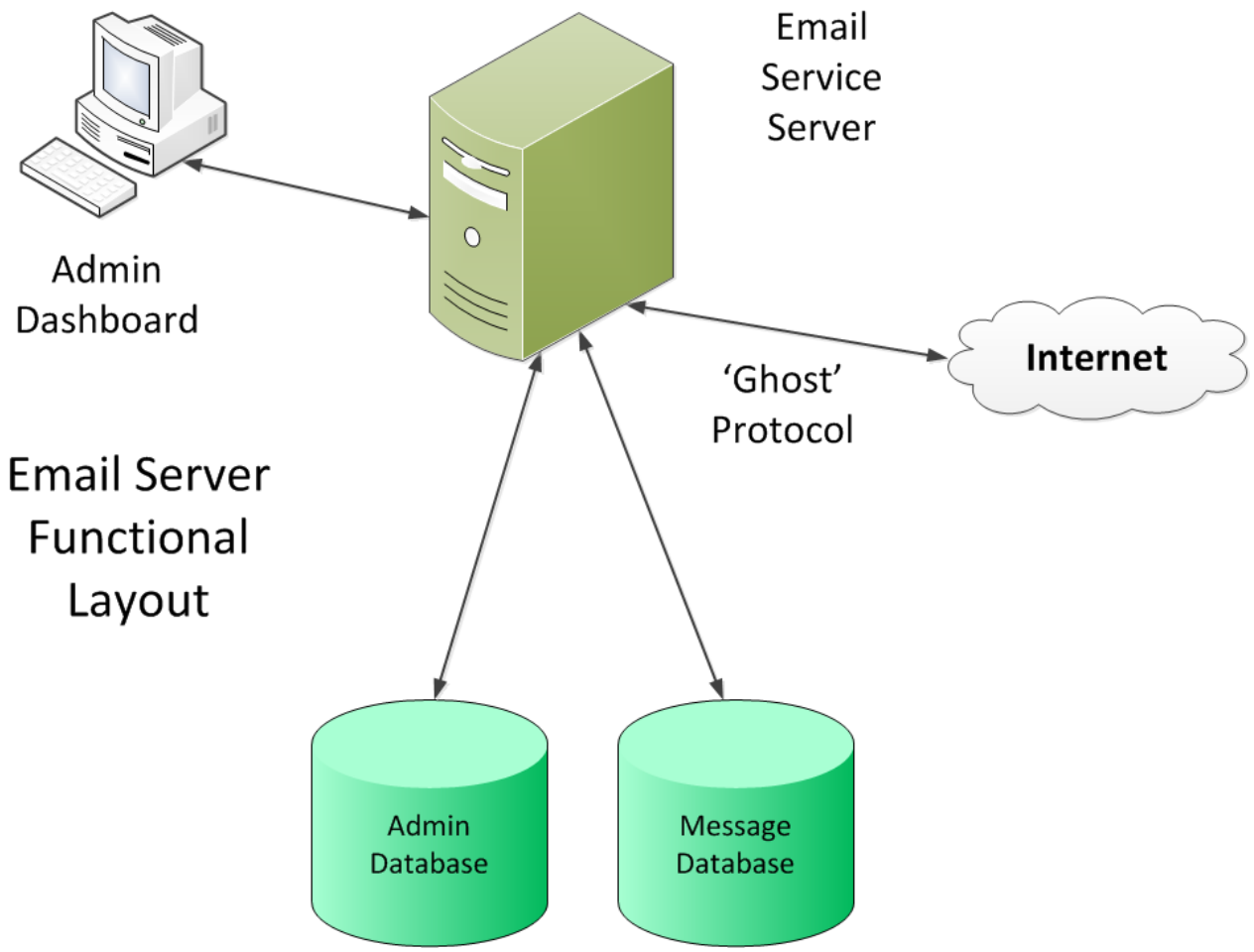
Private Email Server Functional Overview

from

Secure Digital Communications

The **SDC Private Email Server** (PEMS) facilitates secure, private and untraceable email exchange between parties over the Internet. PEMS does not utilize any of the traditional email standard protocols such as POP, IMAP and SMTP. Nor does PEMS use any third party security services such as Key Rings, Digital Signatures, Certificates, hardened secure servers etc. PEMS will only operate with later versions of **SDC Private Email** (PEM).

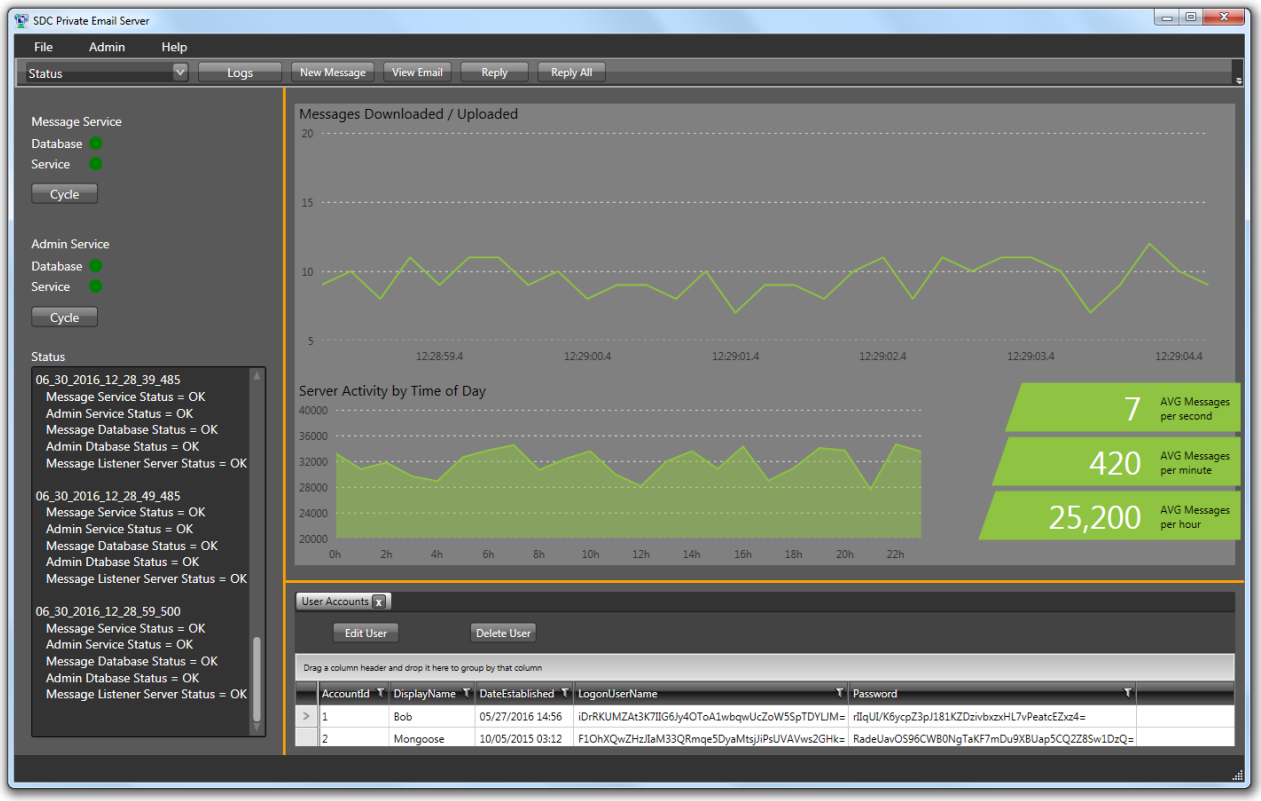
Instead PEMS uses the unique **Point to Point** technology from **SDC Private Messenger** with a new protocol, being developed from the ground up, under the project name of the '**Ghost Protocol'** (GP). An email using GP is sent directly to the PEMS the sender has an account with where it resides encrypted until the recipient retrieves it. There are no email headers on a GP message to parse meta data from if a GP message is sniffed during its ~100 ms life span traversing the Internet. The end goal of GP is to defeat **NSA XKeyscore** and similar operations for end users in the HO/SO environment.



The PEMS is like ordinary email servers in that it receives messages and stores them until the recipient downloads them. After that general description there is little similarity between the two. The PEMS **Admin Dashboard Operator** (ADO) has no way to identify or associate a particular message with an account holder. The GP extends from end user to end user. It does not operate from end user to PEMS to end user.

GP provides for guaranteed delivery much as **Certified Mail Return Receipt Requested** (CMRRR) does in postal system mail. Once a recipient downloads his message and the delivery is confirmed the PEMS deletes it. With GP, just as in CMRRR, there is only one copy of the mail article. This further reduces the target value of PEMS.

The Admin functions within PEMS are part of the GP. The ADO logins into the dashboard with a 256 bit AES encryption key just as in PEM. There is also an internal **Master Key** to facilitate **Key Management** just as in PEM. The GP provides the ADO with special **Key Relationships** with the account holders for admin purposes so that secure, private and untraceable PEMS support issues may be facilitated.



PEMS Admin Dashboard (Prototype)

For further reading on the website: (best viewed with PC or Laptop)

http://www.topsecretcommunications.com/default

Security Overviews for PEM and PM:

http://www.topsecretcommunications.com/HowItWorks

User Guides for PEM and PM:

http://www.topsecretcommunications.com/Support

Additional information:

Stephen Tassio
stephen.tassio@topsecretcommunications.com