

The I.C.E. Box eMail Integrity Assurance Process

eMail Integrity

The combination of message “**validation**” and “**hygiene**” that ensures delivery of all legitimate email with **no spam**, **no lost messages** and **minimized risk** from “malware,” for both **inbound** and **outbound** communications.

The I.C.E. Box “secret sauce”

The Sendio™ I.C.E. Box Service Appliance:

- integrates **standards** such as DKIM and Sender Policy Framework
- uses detailed SMTP **protocol checks** and Sender Address Verification (SAV)
- determines sender **authentication and reputation**, instead of “guessing” about message content

The key validation and hygiene steps

Sender Check: Does the message come from a domain or address that can be verified via a lookup in the global Domain Name Service (DNS) directories ?

- *most spammers are not listed since they do not want to be traced*

Recipient Check: Does the address in the “To:” field actually exist in the email system ?

- *if there is no valid Inbox for the message, then drop it*

SilverListing: Does the sending email server conform to enterprise implementations of the SMTP protocol ?

- *most spammer systems are optimized for high velocity output and do not implement all of the SMTP components*

Anti-Virus: Does the message contain a virus or other “malware” ?

Corporate Policy: Does the message meet defined rules for corporate communications ?

- *no disallowed attachments (eg .EXE or .COM files)*
- *the message cannot be addressed to too many recipients*
- *the message cannot be too large*

Standards Policy: Does the message pass all available Internet standards and services for authenticity ?

- *Sender Policy Framework (Microsoft)*
- *Domain Keys Identified Mail (Yahoo, Cisco)*
- *Commtouch “bulk” message tagging*

Contacts / SAV: Is the sender already known from previous interaction, or will they respond to a Sender Address Verification (SAV) challenge ?

- *include the “human” element to confirm that the sender is not a spam “bot”*

