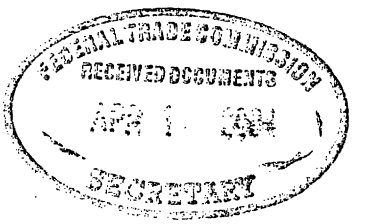
000018

ESPC

Email Service Provider Coalition



March 31, 2004

Mr. Donald S. Clark, Secretary
Federal Trade Commission
CAN-SPAM Act
Post Office Box 1020
Merrifield, VA 22116-1030

Re: CAN-SPAM Act Rulemaking, Project No. R411008
Comments on the feasibility of a Do-Not-Email Registry

Dear Secretary Clark,

On behalf of the Email Service Provider Coalition ("ESPC"), I am submitting the following comments to the FTC in response to the Advance Notice of Proposed Rulemaking for the CAN-SPAM Act. The comments in this letter are specifically related to the FTC's request for comments on the feasibility of a do-not-email registry ("DNE Registry," "DNE," or the "Registry"). The ESPC will be submitting comments on the other components of the ANPR under separate cover.

The ESPC is made up of 48 leading companies – all of which are struggling with the onslaught of spam, as well as the emerging problems related to the deliverability of legitimate and wanted email. Email service providers ("ESPs") enable their customers to deliver volume quantities of email messages. These messages originate from the full spectrum of the US economy. Large and small businesses, educational institutions, non-profits, governmental agencies,

publications, and affinity groups all use the services of ESPs to communicate with their customers, members, and constituents. While ESPs serve the marketing needs of the business community, it is by no means the only customer group served. Email service providers also deliver:

- transactional messages (such as account statements, airline confirmations, and purchase confirmations);
- email publications and newsletters; and
- affinity messages (i.e. alumni bulletins from a university).

It has become quite clear that email is indeed the "killer app." Jupiter Research estimates that the email marketing industry (which, again, is only a portion of the total spectrum of ESPC customers) will grow in size to 8.2 *billion dollars* in 2007. But the size and importance of email in the marketplace should not be measured by dollars alone. Over the past ten years, email has been a strong driver of productivity and efficiency in the marketplace. It has also been an important social tool. Email has shortened distances in the world – allowing communication to occur with unprecedented speed and detail.

These facts point to the critical importance of email in today's world. The ESPC has worked extensively over the past 18 months to ensure that the problem of spam does not threaten the utility of email. And just as importantly, the ESPC has worked to ensure that solutions to spam do not "throw the baby out with the bathwater" and damage the very thing that we are all trying to protect: legitimate email.

Given the prominent status of ESPs in the email industry, the membership of the ESPC has a deep understanding of the implications and effects of the CAN-SPAM Act. Our membership has spent a great deal of time reviewing the Act and the ANPR and we are happy to provide the following comments.

Summary

Under the CAN-SPAM Act, the FTC is required to report to Congress setting forth a plan and timetable for establishing a nationwide marketing Do Not E-mail Registry. Given the recent successful implementation of the national Do Not Call Registry for telemarketing, a parallel to email seems intuitively to make a great deal of sense. Absent a deeper understanding of the technologies, economics and business models involved, one could easily become convinced that a DNE Registry could be an effective solution to the spam problem.

Unfortunately, nothing could be further from the truth. A DNE Registry is a solution that, at best, would be ignored by spammers. At worst, a DNE Registry could cost the marketplace billions of dollars and expose vast numbers of email addresses to more spam. Put simply, a DNE Registry would do nothing to reduce the amount of spam in consumers' inboxes. At the same time the Registry would impede the growth of e-commerce, confuse consumers, and provide a rich source of valid email addresses for spammers and hackers to target.

While we are opposed to the creation of a DNE Registry, we remain committed to finding workable solutions to reducing spam. Promising technology efforts are underway to address the inherent lack of accountability that exists in email transmission protocols. Legitimate email marketers are coming together to create best practices that respect the informed consent of consumers. And consumers are becoming increasingly savvy about the use of email and methods to prevent spam. All of these efforts would become confused or complicated by the creation of a DNE Registry. These solutions are all showing great promise and should be allowed to succeed before a well-intentioned, but ineffective DNE Registry is mandated.

The DNE Registry is Technologically Problematic

1. *SMTP allows for "spoofing" and presents enforcement challenges to a DNE Registry.*

Email is delivered through a protocol called the Simple Mail Transfer Protocol (SMTP). SMTP is indeed a "simple" protocol. It was initially developed in a world without spam and, perhaps as a result, lacks many of the tools necessary to ensure accountability within the system.

SMTP allows the sender of an email to obscure his identity as the message is sent. Further use of open relays (email servers that relay email from any sender) and other technologies allows a sender to hide a true identity completely from the ultimate recipient of the message. This lack of identity in the SMTP system allows spammers to send email with relative impunity. SMTP also already presents an enormous challenge with enforcement of the CAN-SPAM Act, and would only increase under any DNE Registry – for enforcement agencies cannot hold unknown senders accountable. It is indeed true that spammers enjoy the impunity of anonymity.

Spammers seek anonymity to avoid accountability for their practices. The stock and trade of a spammer is a constant search for bandwidth through which to deliver their spam and mechanisms that allow them to hide their true identity. SMTP, through the lack of authenticated identity within the technology, allows this abuse to occur.

Most businesses do not fear accountability. As a result, they do not use the tricks used by spammers to obscure their identities within email. Businesses using email for legitimate purposes generally send email from identifiable email

servers with IP addresses (the Internet address assigned to the server) that remain static. If a legitimate business sends a message in violation of the CAN-SPAM Act, they can quite easily be identified.

The lack of identity (and therefore, accountability) in SMTP presents a daunting challenge to the effectiveness of any DNE Registry. If created, the FTC would be presented with countless violations of the Registry, but would face the near impossible task of identifying the violators (spammers). The expectations of consumers would assuredly not be met as registrations to the DNE Registry would do nothing to reduce the amount of spam received by registrants.

2. ***The technology required for a DNE Registry would be prohibitively expensive.***

One of the largest challenges associated with a DNE Registry is the sheer volume of transactions that would need to occur in order to screen email campaigns against the list. The technological infrastructure costs to support the millions of requests for access to the list would be daunting – and would potentially run into hundreds of millions of dollars.

There are thousands of organizations that use email on a daily basis. Within the ESPC, we estimate that our members provide email delivery services to 250,000 senders within the United States. It is reasonable to assume that each of these senders would need to access the DNE Registry on a regular basis to suppress registered addresses from their lists (daily access would probably be necessary).

Again in contrast to telemarketing, consumers generally have more than two email addresses. And each member of a household is likely to have multiple email addresses – meaning that every household could have numerous email addresses (whereas most households have less than two phone numbers). It is reasonable to assume that the DNE Registry would quickly grow to twice or three

times the size of the Do Not Call Registry – meaning that between 100 and 150 million email addresses could be added to the Registry in short order. The size of the Registry would be multiplied over time as email addresses are frequently discarded as consumers move jobs, change ISPs, or simply change their email address. Even more so, ISP's and business often 'recycle' old email addresses to new users, which could further degrade the effectiveness of the registry. It is possible that the Registry could grow to over 500 million email addresses within two years if proper maintenance was not performed on the list.

The processing demands associated with over 250,000 senders accessing a Registry that contains between 100 and 150 million email addresses are prohibitively enormous. The cost for the systems required to support such processing is too expensive to justify the benefit. And it should be noted that these costs would be borne heavily by the organizations that need to access the Registry – for they, too, would need to add capacity to support the processing necessary to cleanse lists.

3. The Registry Would Represent a Single Point of Failure for Email

If a Registry were created, it would present an unacceptable single point of failure to the legitimate businesses that would need to rely on the system. Put simply, the use of a centralized Registry would result in every email marketer being reliant upon the continued functionality of the Registry. Any downtime in the Registry (and such downtime must be expected) could seriously delay or prevent the delivery of legitimate email messages.

It is possible that the Registry would become a target for attacks by spammers and hackers. There are precedents for such attacks being launched against anti-spam efforts. Last year, many of the anti-spam blacklists were disabled due to attacks against the systems used to maintain and distribute the blacklists. Such

attacks can be expected to occur upon a DNE Registry – raising the risk of failure of the Registry system.

4. The Registry Would Present an Unacceptable Security Risk

Of all the technological challenges associated with a Registry, one emerges as the most compelling reason to not create a Registry: security. As discussed above, the Registry would quickly grow to include millions of valid email addresses. Such a list would represent the richest source of "live" email addresses ever created. The temptation to technologically-savvy spammers would be undeniable. The Registry would immediately become one of the most visible and coveted targets for spammers and hackers to infiltrate.

Also discussed above was the fact that the Registry would present a single point of failure in the email system. This reality exists with regards to security as well. A centralized Registry would present a single point of failure for the integrity of the email addresses held within the Registry. A single breach of the Registry's security would expose millions of email addresses to vast quantities of spam. And, once the Registry were breached, the email addresses within the Registry would have no protection and would be freely shared and circulated amongst spammers – resulting in even more spam for the registrants. Once these addresses are in the marketplace, the registry would be immediately deemed ineffective, and potentially every registrant would need to change their email address.

There are encryption tools that could be used to improve the security around a Registry. However, history has shown that the best security is still subject to failure. While it is possible that adequate security could be created to protect the Registry from the risks that exist today, it is not possible to ensure the continued viability of such protections in the future. And the risk of a breach (compromised

email addresses for all those who registered) is too high to warrant the creation of a Registry.

5. Promising Technological Solutions to Spam Are Under Development and Should Be Permitted to Succeed Before a Registry Is Mandated.

The lack of accountability is a well-recognized problem in email. Many efforts are underway to build authenticated identity into the infrastructure of email technology. As discussed above, spammers enjoy the impunity of anonymity. We could begin to hold spammers accountable for their actions if we could take away anonymity in email (through authenticated identity). The ESPC has been a leader in the development of such solutions. In 2003, the Coalition released a whitepaper to outline the ways through which authenticated identity could be accomplished within email. A copy of the Project Lumos whitepaper is attached as Appendix A.

Since the release of Project Lumos, there has been significant activity around authenticated email. Microsoft has proposed "Caller ID," Yahoo has released "Domain Keys," and AOL is testing "SPF." All of these solutions involve the authentication of some component of the email being sent. And while still in development, these efforts offer promising hope for solutions to spam and should be permitted to succeed before a DNE Registry is mandated.

A DNE Registry Would Not Be Effective in Reducing Spam

1. Spammers Would Not Comply with a DNE Registry.

One of the largest problems associated with a DNE Registry is the simple fact that it would not be effective in reducing spam. We know conclusively that spammers do not take heed when new laws are passed. The 37 state laws

previously in place would have been effective if spammers were inclined to comply with legal requirements. The passage of the CAN-SPAM Act provided state AGs and the FTC with important enforcement tools, but spammers still have not heeded the rules governing email.

We should not assume that the creation of a DNE Registry will see any different result. Spammers will continue to be anonymous and hide behind open relays and spoofed identities. It should also be noted that many spammers operate from overseas locations, beyond the reach of domestic enforcement. As long as they can obscure their identity and hide offshore, spammers will continue to ignore legal requirements, including a DNE Registry.

If spammers will not abide by a DNE Registry, the amount of spam will not decrease. And that raises a fundamental question: why create a DNE Registry if it will not result in a decrease in the amount of spam? Clearly, we should not pursue an expensive and security-impaired solution without a very strong indication that it will achieve the desired effect of reducing spam. A DNE Registry fails this test.

2. Spammers Are Already Violating the Law.

In a 2003 study, the FTC found in a random survey of 1000 pieces of spam that fully two thirds of the email reviewed included some indication of falsity.[1] This statistic is borne out by a review of any email inbox: spam is based upon falsity and fraud. Spammers are thus already violating the law. Their messages are presumably in conflict with existing consumer protection standards at both the state and federal levels.

The CAN-SPAM Act adds more tools for enforcement agencies and clarifies that some practices are indeed illegal (such as harvesting email addresses, creating

[1] "False Claims in Spam," A Report by the FTC's Division of Marketing Practices, April 30, 2003.

multiple email accounts for purposes of spamming, or falsifying header information). Yet spammers continue to ignore these standards.

We cannot assume that spammers will comply with a DNE Registry. Indeed, we should assume that they will not. Spammers are already violating the law and will continue to do so under a mandated DNE Registry.

The creation of a DNE Registry will divert resources from important enforcement actions under the FTC Act and the CAN-SPAM Act. These existing laws should be enforced vigorously and allowed to achieve the full measure of their intended purpose before a DNE Registry is considered.

3. Legitimate Email Marketers Are Not Spamming.

The use of email by marketers has proven to be a powerful and effective tool in the marketplace. But abusing the interests of consumers is not effective. Marketers that intend to be in the marketplace over time cannot afford to spam their potential or existing customers. Indeed, the effects of ISP filtering due to consumer complaints can threaten the viability of a marketer if they do not respect consumer concerns in the execution of their email campaigns. Legitimate email marketers have enormous incentives to deliver email that complies with the expectations of the recipient.

Given this reality, the marketplace has responded with best practices that respect the consumer's inbox. Increasingly, legitimate email marketers are delivering messages only to recipients that have provided informed consent to receive email. The ESPC released a "pledge" for members in 2003 (attached as Appendix B) that requires that "unsolicited commercial email shall not be sent." The need for informed consent prior to delivering marketing messages via email has become a business imperative for legitimate companies.

It follows that a DNE Registry is unwarranted if spammers are going to ignore the Registry and legitimate email marketers are obtaining the informed consent of recipients prior to sending email. Again, for what purpose would a Registry be created if those to whom the Registry was targeted would not participate?

A DNE Registry Would Present Enormous Implementation Challenges

1. *Confusion Would Be Created as to What Messages Must Be Screened Through the Registry.*

One of the major differences between telemarketing and email is the breadth and variety of messages transmitted. Telemarketing was exclusively the domain of marketing messages. Email is used to deliver a multitude of messages of every conceivable variety. Newsletters, account statements, personal communications (including one-to-one marketing or advertising), transaction reports, and affinity messages (such as alumni bulletins from a college) are all delivered through email. Many of these messages also contain promotional or advertising material. In some cases, the promotional content is significant and is used to support the primary purpose of the email (*i.e.*, newsletters).

Parsing these various communications to determine what would be subject to the Registry would be a daunting and confusing task. A DNE Registry would need to have an exhaustive list of exceptions to cover the messages that consumers expect to receive even after their email address is registered.

2. *The DNE Registry Would Need to Include Volume Triggers, Further Complicating Implementation.*

The CAN-SPAM Act does not include any volume triggers for compliance with the Act. In other words, a single non-compliant email can result in exposure

under the Act. While this is a concern under the CAN-SPAM Act generally, volume triggers would be an absolute necessity under a DNE Registry. But tracking volume and ensuring compliance would be a nearly impossible task under a mandated DNE Registry.

Many unsolicited commercial email messages are personal communications. A local real estate agent may send an unsolicited email to a homeowner considering selling their home. Or a branch loan officer may learn that someone in their town is looking for financing and send an email introducing their services. Each of these communications is an unsolicited commercial email message. Yet each message was sent only as a single communication to a single recipient.

The CAN-SPAM Act does not include any exemptions for low-volume or personalized messages. As a result, single emails (as described in the examples above) can create exposure for the organizations sending the messages.

A DNE Registry would need to exempt low-volume or personalized messages. Failure to do so would have catastrophic effects on the free flow of communication at a local and personal level. Large organizations would need to filter all outgoing email communications – including messages sent by local employees to individual prospects – through the DNE Registry. This would delay and burden the growth of email as a powerful communications tool.

3. A DNE Registry Would Disproportionately Harm Small Businesses.

Much commercial email is sent from small businesses. The power and simplicity of email communication has not been lost on the millions of smaller organizations around the country. For most of these organizations, technological resources are limited. Email works for them because it is cost effective, simple, and successful. Adding a DNE Registry to their obligations would present daunting resource challenges and may result in a migration of small business *away* from email.

As discussed above, the technological challenges of a DNE Registry are overwhelming. Sophisticated security systems and file sharing mechanisms would need to be used to prevent abuse. These same safeguards will present an insurmountable challenge to small businesses with limited technology expertise. Small businesses will not be able to incorporate the required security into their operations in a cost-effective manner. Indeed, small businesses may not be able to support the costs associated with implementing a DNE suppression process, period. This dynamic could have the harmful effect of disproportionately forcing small business away from email as a marketing tool.

Comparisons to the Do Not Call Registry Are Inappropriate

One of the drivers for the inclusion of a DNE Registry study within the CAN-SPAM Act was the tremendous popularity and successful implementation of the FTC's Do Not Call Registry for telemarketing (the "DNC Registry"). It intuitively follows that a DNE Registry would be similarly popular and easily implemented. But such intuition is flatly incorrect. Email differs markedly from telemarketing. An understanding of these differences leads to a clear understanding: a DNE Registry would not work for email marketing.

1. Telemarketers Are Identifiable and Accountable, Spammers Are Not.

As discussed above, spammers send their messages with the impunity of anonymity. Spammers can abuse SMTP to obscure their true identities. As a result, they remain unaccountable for their actions. In contrast, telemarketers are fairly easy to find – they can be tracked by the phone number from which they are calling.

Accountability must be a condition precedent to the creation of a DNE or DNC Registry. We have accountability in telemarketing due to our ability to track

phone numbers. We do not have accountability in email due to the ability of spammers to spoof their identities. As a result, a DNE Registry does not allow for effective enforcement, while a DNC Registry can be very effective.

2. *The Cost of Creating and Sending a Message Is Very High in Telemarketing and Very Low in Email.*

To engage in telemarketing, telemarketers must invest heavily in the actual transmission costs of their messages (the toll for the phone call). They must also pay for the human resources to actually make the calls. Again in contrast, the costs to create and deliver an email message are very low. A spammer can send millions of messages with negligible technological and human costs.

As a result, telemarketers have a compelling incentive not to call those individuals who do not wish to receive calls. It simply costs too much to make a call that has no chance of success. In contrast, spammers have every incentive to ignore the interests of recipients. For a spammer, volume does not increase costs dramatically. In fact, for a spammer, volume is critical – as the response rates to spam are infinitesimally low.

Thus, a DNC Registry works for the telemarketing industry – telemarketers have a strong economic incentive not to send messages to people on the DNC Registry. But a DNE Registry would prove ineffective in stopping spammers, as they have no economic incentive to reduce the volume of their messages.

3. *Vast Public Records of Telephone Numbers Currently Exist, Similar Email Records Do Not.*

The majority of personal telephone numbers in the United States are available through public directories (phone books). As a result, it is fairly easy to find the

listed phone number for any person in the country. The cost of creating and transmitting a phone call helps to prevent the abuse of these public listings.

In contrast, email addresses are not included on any master directories. An email address is, currently, a private identifier that is disclosed at the discretion of the owner. This system is logical given the abuse that would occur if a large directory of email addresses were created. The comparative lack of economic inhibitors to volume email would see spammers immediately abusing such directories if they were to be created.

The creation of a DNE Registry raises unanswered concerns about aggregating vast numbers of email addresses in a single location. We simply cannot afford the risk of abuse of such a list where the cost of sending millions of email messages is so low. A DNC Registry presents no additional risk to the numbers listed in the DNC Registry (they are already available publicly already). A DNE Registry presents enormous risks to the email addresses listed in the DNE Registry, as no such directory otherwise exists.

Conclusion

A Do Not Email Registry is intuitively a compelling tool to reduce spam. But the reality is that a DNE Registry will create far more problems than it actually solves. The costs to business and the public to build the infrastructure necessary to support the sheer volume of transactions through a Registry will be staggering. The potential security exposure associated with the world's largest directory of email addresses is simply too risky to condone. And most importantly, a DNE Registry will do nothing to deter spammers! Consumers registering to the list will not see any decrease in spam and may, in the event of a security breach, see much, much more junk email in their inboxes.

There is significant work being done in the marketplace today to respond to spam. Legitimate businesses are defining best practices that respect the informed consent of consumers. Important studies are showing consumers how to properly safeguard their email addresses to prevent spam. And technology is being developed to bring accountability into the email system. A DNE Registry would take scarce resources away from these important efforts. For these reasons, we strongly urge the FTC to counsel Congress on the threats and problems associated with the DNE Registry.

Sincerely,

Trevor Hughes
Executive Director
Email Service Provider Coalition

Appendix A

Project Lumos:

A Solutions Blueprint for Solving the Spam Problem by Establishing Volume Email Sender Accountability

White Paper
September 24, 2003

Issued by the

Network Advertising Initiative
Email Service Provider Coalition

Abstract: Unsolicited commercial email, or spam, is an overwhelming problem for consumers, businesses, non-commercial organizations, and Internet Services Providers. A cornerstone to solving the spam problem is to hold email senders accountable for the mail they send and their sending practices. This white paper proposes a federated Registry model for registering and certifying volume email senders. The proposed federated Registry will provide services to ensure a secure representation of the sender's identity, adherence of the sender to applicable public procedures and policies, and assessment of the sender's performance. By including the Registry information in the SMTP mail header of certified email, receiving email gateways can make more accurate and consistent decisions regarding the processing of incoming email.

Authors:
Hans Peter Brondmo
Margaret Olson
Paul Boissonneault

1. Executive Summary

Unsolicited commercial email, or spam, is consistently identified as one of the primary issues for consumers, businesses, non-commercial organizations, and Internet Services Providers (ISPs). Spam represents a substantial proportion of the billions of emails sent each day, and the volume of spam is increasing exponentially. A recent analysis from Brightmail suggests that by September 2003, as much as 50% of all email will be classified as spam by the recipient. Some ISPs report that spam is already exceeding this level by a considerable amount.

The volume of spam adversely effects recipients of the email and the providers of email services. All organizations that receive mail - ISP's, businesses, governments, and institutions – are experiencing rising costs as the magnitude of email continues to increase. Spam impacts employee productivity by forcing employees to sort through their inboxes for pertinent communications, and systems administrators are fighting a losing battle in their attempt to stem the spam flood before it reaches individual mailboxes. To many individuals, the incidence of pornographic spam to their inboxes is offensive, and could represent a legal liability to organizations. Lastly, spam is frequently the medium used to defraud consumers and steal personal and financial information. While quantifying the cost of the effects of spam is difficult to measure, it is unquestionable that spam threatens the trustworthiness and viability of email and eCommerce.

In an effort to curb unwanted and offensive email, organizations and individuals have implemented anti-spam measures that include blacklists, whitelists, and content filters. These solutions are fundamentally heuristic and have their own inherent problems. Anti-spam measures are not perfect in their ability to distinguish spam from legitimate email. A study by Assurance Systems in the fourth quarter of 2002 found that the top 10 email account providers' spam detection software incorrectly identified an average of 15% of legitimate email as spam and consequently did not deliver it to the inbox.

Because Simple Mail Transfer Protocol (SMTP) is not secure, it is exploited by illegitimate bulk mailers to obscure their identity and forge their email headers. Illegitimate mailers are thereby able to send millions of fraudulent spam messages with indifference to any repercussions.

The flexibility of email content and origin in the current infrastructure, combined with the heuristic nature of the current spam fighting tools, results in a never-ending cat and mouse game of attempts at detection by the spam solutions and deception by the spammers.

This white paper presents a blueprint for an extension to the existing email infrastructure that aims to eliminate spam by holding high volume senders and Email Service Providers (ESPs) accountable for the mail they send and their sending practices. Project Lumos proposes the establishment of one or more federated Registries to provide certified sender identity and performance reputation information to receiving email gateways. By providing identity and reputation information, receiving email gateways can make more accurate decisions about how to process incoming email.

There are three key aspects proposed in the Project Lumos architecture.

I. One or more federated Registries that provide:
- Certification for high volume email Senders and ESPs upon verification of identity. Upon certification, the Registry issues the Sender or ESP a secure identity. The secure identity is a set of electronic credentials based on Public Key Infrastructure cryptography that can be used to authenticate the source and content of email.
- Volume Email Standards for bounce handling, abuse report handling, unsubscribe handling , and similar technical standards.
- Reputation Services that link identity information to performance data, and an objective Performance Rating. This information would be available to anyone who requests it.

II. Volume email processing provisions for:
- Enhancement to email headers (new X-Headers) to include identity and other information required to securely distinguish the sender and support the reputation engine.
- Enhancements by receiving Email Gateways to utilize the modified email headers, validate the email source, and check the objective Performance Rating of the Sender and ESP (from one or more registry sources).

III. A set of standards for reporting reputation data and scoring, including:
- A mechanism for collecting and reporting the raw performance data for senders and ESPs. Raw performance data includes incoming volume, hard bounce counts, unsubscribe requests and complaints as seen by the Receiving Email Gateway.
- A Performance Rating service to calculate performance ratings for registered entities.

Each of these aspects is further described in the body of this white paper along with proposals for the implementation of certification and classification schemes, volume email standards, and an illustrative example of performance measurement and rating algorithms.

With access to the secure identity information, performance data, and performance ratings from a Registry, the recipient organizations' email gateways can implement rules and make decisions with regard to processing incoming email. Based on the sender's reputation, email gateways have the option of passing email freely, subjecting it to a series of anti-spam filters, routing mail to a bulk mail folder, or blocking the email altogether.

All of the technologies required to implement this proposal exist today. Implementation will be phased in over an approximate 18-24 month timeframe. Phase 1 entails commercial high volume ESPs publishing their mail server IP addresses and providing the new X-Headers. This affords crude measures of performance, and provides a minimum level of identity. Phase 2 sees basic sender and server certification, and secure identity services established. Performance tracking will be implemented in Phase 3. And Phase 4 incorporates the more detailed aspects of certification and mail categorization.

A few key outstanding questions must be addressed prior to implementation. First, who will own and operate the Registries and under what business model? Second, is there a requirement for an external organization to oversee the operation of the Registries and provide a dispute resolution mechanism? And lastly, how will Project Lumos work with the appropriate bodies to create the standards necessary to ensure effective definition and communication of the identity and performance data?

The Network Advertising Initiative (NAI) Email Service Provider Coalition (ESPC) has no current plans to implement this solution on its own, but is offering this blueprint as a framework around which a solution can be built. This white paper calls for broad participation and feedback on the proposed framework and the detailed aspects contained herein.

Introduction

2.1 Paper Objective

This white paper describes a systems architecture approach to solving the growing spam problem by making modifications to how high-volume senders and receivers of email interoperate. The architecture consists of a set of federated registries responsible for implementing and operating the proposed solution.

2.2 The Problem with Identifying Spam

Spam filtering as it exists to today is imprecise. Not only does it fail to catch a great deal of spam, and incorrectly mark legitimate email as spam, current spam filtering solutions are unable to verify that the mail was actually sent by the sender that is identified in the email. Further, maintaining spam filter settings on requires constant attention because spammers continuously change their practices to circumvent filtering tools.

The use of email filtering software is a widely accepted tool for distinguishing spam. Email filtering software (at the incoming mail gateway and/or the user's personal computer) applies content and header-based analysis rules to identify spam and remove it from the system. However, cleverly written emails often evade the logic of the software, and configuring the filters to catch spam without a percentage of false positives is impossible.

Organizations also use 'blacklists' or 'blocklists' of IP addresses compiled by members of the Internet community to identify potential spam sources. The receiving mail gateways are configured to block all mail from these sources. However, even the operators of these lists acknowledge that blacklists are imprecise and can result in blocking email from legitimate senders and IP addresses. The outcome of blocking legitimate senders and IPs is collateral damage, or put more plainly, wanted email does not get delivered to the intended recipient.

If the ability to evade these filtering techniques isn't enough, the current Simple Mail Transfer protocol (SMTP), by design, is not secure. SMTP makes it easy for illegitimate bulk commercial mailers to use technology to forge email headers and obscure their identities. Spammers routinely misrepresent the email sender information in the SMTP headers, and may even lie about their identity in an attempt to get their messages delivered.

Information falsification combined with the use of 'open proxies', further enables illegitimate senders to conceal their identities. By accessing incorrectly configured email servers or computers hijacked through viruses or by hacking, spammers send millions of anonymous spam messages.

It's time for legitimate senders who have nothing to hide to stand up and identify themselves so that the those who have built their business on 'tricking' spam detection mechanisms can no longer operate in the dark.

2.3 Terminology and Definitions

The following terminology is used throughout this white paper:

- Sender - The term 'sender', when used with respect to a commercial electronic mail message, means an organization or person who initiates such a message and whose product, service, or

[1] Press Release, see http://www.brightmail.com/, Brightmail, San Francisco, CA, July 1, 2003.
[2] Fourth Quarter Email Blocking and Filtering Report, see http://www.assurancesys.com/, Assurance Systems, Superior, CO, Feb. 2003.

Internet web site is advertised or promoted by the message. The Sender is usually designated by the "Mail From:" line in the email header.

- Mail Server – The term 'mail server' is used to designate the physical machine that sends the email (the MTA or Message Transfer Agent).
- Email Service Provider – The term 'Email Service Provider", or "ESP", is used to represent the Sender's agent, the organization which operates one or more mail servers. The ESP may be a separate group within the Sender's own organization (such as an IT Department), an ISP, Web mail provider (such as Yahoo, MSN, AOL, etc.), a public mail list operator, or a commercial email services provider (such as a member of the ESP Coalition listed in the Appendix).
- Recipient – The term 'Recipient', when used with respect to a commercial electronic mail message, means an authorized user of the electronic mail address to which the message was sent or delivered[4].
- Receiving Email Gateway – The term 'Receiving Email Gateway' or 'Gateway' is used to designate the machines that receive the email. This can be a single machine or an installation consisting of firewalls, filters, servers, etc. ISPs, enterprises, or other organizations operate gateways on behalf of the email recipients.
- Identity – The term 'Identity' is used to describe the verified and certified unique identification of a person, commercial organization, or non-commercial organization.
- Reputation – The term 'Reputation" describes a measure of the overall quality of a Sender or ESP as judged by the external community. The reputation of senders is largely established by the email recipients.
- Campaign – The term 'Campaign' designates a unique volume email occurrence from a particular Sender and/or ESP to a broad range of recipients.
- Unsubscribe – The term 'Unsubscribe' designates a request from a recipient to no longer receive any mailings (on any topic) from a particular Sender.
- OptOut - Unsubscribe
- Registry – The 'Registry' designates an organization that provides an email sender reputation engine, certification services, and publishes a set of standards that it enforces on all registered senders.
- Internet Email Trust Authority (IETA) – a Registry

2.4 Project Lumos Solution Overview

In today's environment, it is expensive for mail gateways to monitor incoming email and determine what is legitimate mail and what is spam. While the largest mail gateways (large ISPs) have dedicated resources to this task, smaller ISPs and mail systems administrators do not always have the knowledge or the resources to manage the task. Project Lumos proposes the establishment of a federated model of registries to implement sender accountability. By mandating that senders provide certified proof of identity to the receiving email gateways, in addition to providing historical performance measures about the sender, any recipient can confidently decide what email they want to receive and what email they do not want to receive.

The role of Registry is to verify the identity of high volume email senders and ESPs, and issue electronic credentials that allow receiving mail gateways to authenticate mail coming from the certified sender or ESP. As part of the terms of registration, a Registry will also require that senders and ESPs commit to adhering to a set of well defined, public Volume Email Standards and procedures. The Registry also creates and maintains an electronic record of the sending organization, including its sending policy statement, in its public Registry. Figure 1 shows a high level functional view of a Registry.

[3] S.877 CAN SPAM Act of 2003, section 3, introduced to the US Senate April 10, 2003.
[4] Ibid.

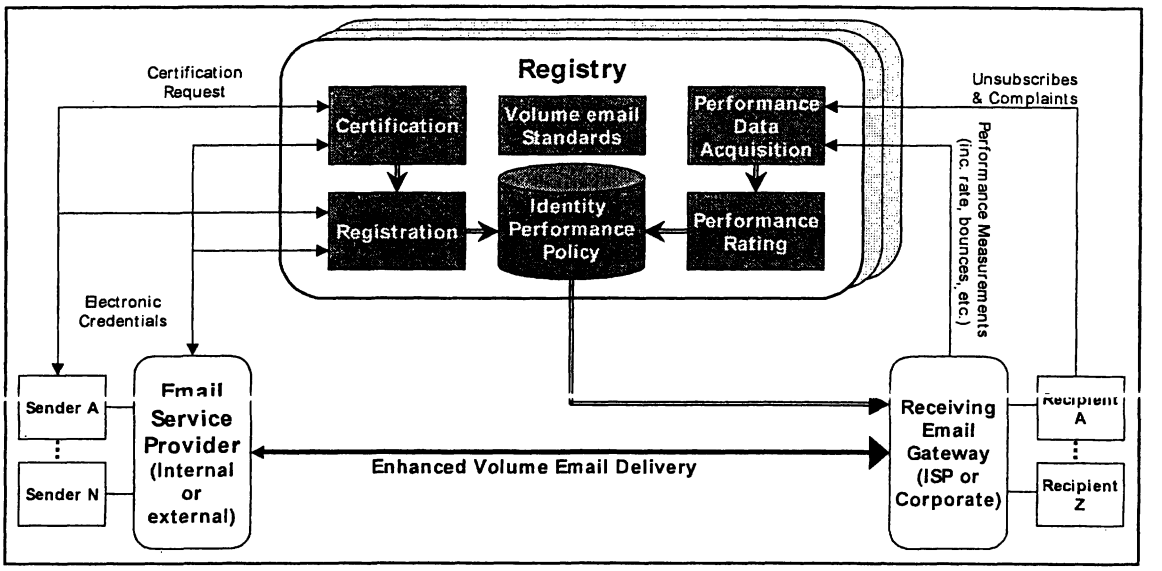


Fig. 1 – Functional View of the Registry Model

In addition to establishing Registries, Project Lumos proposes enhancements to the Volume Email Delivery process that will introduce a secure method of including the sender and ESP identity in the email header. By providing this information in the email header, receiving email gateways can validate the source of the email. These enhancements can also be used to authenticate the content of the email, and communicate permission-oriented information such as trusted unsubscribe and abuse reporting mechanisms.

The final component proposed by Project Lumos is a process to monitor and report the performance of registered senders and ESPs. Data from receiving email gateways will be combined with information from recipients about abuse complaints and repeat unsubscribe requests. This information will be used to objectively rate the performance of the registered senders and ESPs.

A good reputation, as demonstrated by a high performance rating, can only be established through consistently good behavior. Since reputation is linked to identity, Project Lumos encourages senders to maintain their identity. The coupling of identity and reputation is therefore critical to ensuring that senders and ESPs don't attempt to defeat the system by "churning" identities.

Implementing the proposed federated Registry model requires an open, decentralized physical architecture and inter-operable standards for information sharing. It is not merely a point solution. The Blueprint first assumes that there will likely be multiple implementations of Registries, and second, that the different functions of a Registry may be implemented and operated by separate organizations working in partnership.

2.5 White Paper Outline

Section 3 presents a deeper look at the requirements for a solution to the problems created by spam. This is followed in Section 4 by a description of the proposed technical solution for the overall architecture and the key components. Section 5 presents a workable, phased implementation or transition plan to implement the blueprint, and Section 6 contains conclusions and identifies next steps required for the implementation.

Appendices provide acknowledgements, a list of resources and information about other complementary initiatives, additional information about the NAI ESPC, contact information, and a concise set of FAQs about the blueprint.

Business Requirements for a Solution

3.1 Accountability

Any comprehensive solution to the spam problem requires that email recipients be able to hold senders and ESPs accountable for the quality of their email. Senders and ESPs who establish a good reputation (i.e. a high performance rating) will be trusted and their email will be routed to recipients. At the same time, volume mail from unknown senders, known senders with no demonstrated performance, or those registered senders who have exhibited poor performance, will be held accountable for their past behavior and subjected to additional filtering or even blocking of their mailings.

In order to achieve this accountability, a complete solution must:

- Eliminate the ability for high volume senders to hide their identities,
- Provide a secure mechanism for validating the sender of incoming email,
- Ensure that a certified sender's identity may not be impersonated nor their content modified by an illicit third party,
- Establish minimum volume email standards (volumes, bounce rates, bounce handling, etc.) to which registered senders and ESPs must adhere,
- Provide a mechanism for monitoring sender and ESP compliance with contractually binding standards by tracking their performance and determining an objective rating of performance,
- Allow Email Gateways access to sender and EPS identity information and performance ratings to use in implementing its local delivery policies,
- Place no burden on small, anonymous senders,
- The architectural changes must allow for transparent inter-working with senders who are not registered, and
- The architectural changes must allow for transparent inter-working with email gateways and pre-existing technology solutions that do not to implement identity or reputation checking.

The following sub-sections define each of these high level requirements in more detail.

3.2 Secure Identity of the Sender

3.2.1 Sender Certification

Through the sender certification process, high-volume senders and ESPs are required to authenticate their identity and commit to follow acceptable industry guidelines for sending volume email.

Specific requirements of certification include:

- Volume email senders and ESPs provide legal proof of identity.
- Certification is available at different levels, depending on the intended volume of email and degree of certainty that a sender's ID can be authenticated. Some Registries may choose to implement only certain levels of certification.
- Senders and ESPs contractually commit to the Registry's volume email standards as part of the certification process.
- Approved senders and ESPs are issued 'electronic credentials' that certify their identity.
- The certification process must not be cost prohibitive to small businesses and small, non-commercial list servers.
- Electronic credentials can be revoked should they be compromised.

3.2.2 Sender Identity

Intuitively, sender identity is a simple idea – it is a person or organization that is responsible for the creation and initiation of email content, or who is facilitating email delivery. Perusing an inbox may reveal senders such as 'Bob Smith', 'orders@redenvelope.com', 'Origins Online', 'United Airlines', or 'Nordstrom'. The Lumos sender identity is intended to make those identities secure, so that the recipient can be confident that the sender is who they say they are.

Despite the simplicity of the sender identity concept, determining level to which assign sender identity and performance ratings is not so simple. Large organizations often operate in a decentralized fashion, with different divisions publishing their own documents. For example, AOL Time Warner includes brands such as AOL and "This Old House". How many TOH newsletter recipients know, or care, that the TOH website is owned by AOL Time Warner and not the television station that produces the show? Does the performance of the TOH email get attributed to TOH? AOL? Time Warner? All of the above?

The structure of the Identity, and the resulting certification process, must provide for Certification of the corporate Identity at the highest level, in addition to individual identities to be issued within the context of the corporation. Similarly, the system must be flexible enough to measure the performance of an individual "division", and to aggregate all "division" performance ratings to an aggregate organization performance rating. This encourages the overall organization to exert some control over their departments and subsidiaries.

A hierarchical Identity structure is required to meet the above requirements. The structure should allow for an arbitrary number of levels in an "identity tree". For instance, an organization may have as many sub-identities as they want, but they are all tied to the top-level identity. Each sub-identity will have its own Reputation or performance rating, while the top-level identity's performance rating is the combination of its sub-identities. An example of a three level identity structure is shown in Fig. 2.

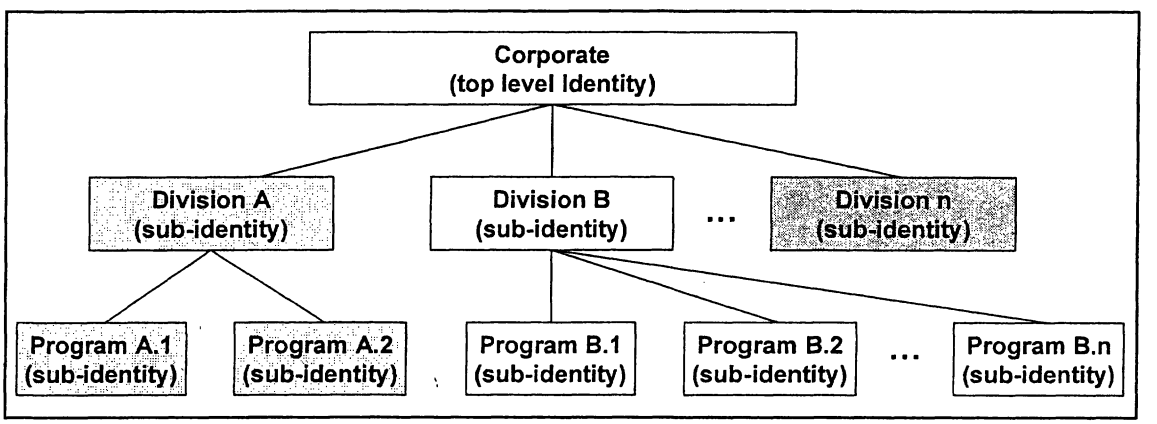


Fig. 2 – Example of a Hierarchical Identity Structure

To prevent churn and disposal of sub-identities with poor performance ratings, sub-identity ratings cannot be removed from the top level rating until they have been dormant for an extended period (e.g. three years). In a large organization one wayward division is unlikely to overly harm the overall rating, but allowing poor performers to repeatedly obtain a new identity and repeat the inappropriate behaviors, will eventually impact the corporation's overall reputation.

3.2.3 Individual and Anonymous Senders

The Internet has been the great equalizer – individuals can now communicate over long distances where the previous alternatives were either slow or expensive or both. With anonymity, free (or freer) speech is available to far more people than it has at any time in the past. These valuable features must be preserved.

Small and anonymous senders are sending via some sort of ESP – be it their corporate gateway, an inbox provider such as Yahoo or HotMail, or a broadband or dial-up provider. For these senders, there is no individual reputation but their identity is marked as low volume by their ESP. Recipients can therefore trust that the email from such an individual is extremely unlikely to be spam.

In all cases, the sender has some sort of account with their provider. Under the Lumos scheme, the ESPs are rated. To maintain their rating, service providers to small and anonymous senders limit their members to a number below which sending spam is not cost effective. A limit of, for example, 100 messages per day is a very large number for an individual, but an inconsequential number for a commercial message of any kind.

Currently, providers of free or low cost mailboxes and mailing services have a variety of fraud prevention mechanisms that prevent individuals from abusing their systems by sending large volumes of email for little or no cost. These fraud prevention systems will now have an additional incentive – allowing abuse will not just eat up bandwidth, but will threaten the service provider's reputation rating, which in turn will threaten the viability of their service for all of their customers.

3.3 Objective Performance Rating of Senders and ESPs

The definition of 'spam' and what comprises acceptable permission to send email has been the subject of much debate, yet the industry remains no closer to a consensus definition. Ultimately, spam is in the eye of the Recipient and is extremely context sensitive ... 'that which I do not wish to receive is spam'. Any solution to spam must leave ultimate control to determine what they do and do not want to receive up to the recipient. By creating an objective rating mechanism on a known scale, Project Lumos avoids the black/white labels that have proven to be unmanageable and impractical. As the rating system evolves, senders and ESPs will develop best practices that their recipients find acceptable. These practices may be different for different uses of email, in different markets, or for different recipient communities.

In order to establish the performance of senders and ESPs, a mechanism must first be established for capturing performance data. Second, a service must be established in order to make the aggregate performance data and ratings available to email gateways. These functions may be performed by Registries or may evolve as a separate, third party services. The following two sections describe some of the requirements for capturing performance data and rating senders.

3.3.1 Capturing Performance Data

Continuous performance measurement is required to establish the reputation of both senders and ESPs.

Therefore receiving email gateways will:

- Measure performance of incoming mail streams including the following information:
  - Email rate and Volume;
  - Bounce rates and handling;
  - Presence and accuracy of the additional information required in headers.
- Report performance data for senders and ESPs to their certifying Registries.
- Route (redirect) unsubscribe requests to the Registry prior to being forwarded to the sender (thus allowing automatic monitoring of unsubscribe request handling).
- Copy Abuse reports ('spam reports' from end recipients) to the Registry as well as the sender or ESP.

3.3.2 Performance Rating Services

Performance ratings will be generated and published based on aggregated information from a number of email gateways. In order to accomplish this, a performance monitoring service must:

- Ensure that it can accept the performance information from a wide number and variety of gateways.
- Continually produce and update the performance ratings of registered senders and ESPs.
- Design and implement a rating algorithm such that higher performance ratings will be earned as the senders or ESPs demonstrate good performance over time, similar to a consumer's credit rating.
- Include a "damping function" in the rating algorithm so that more recent events have a higher importance than past history. The weight of historical performance nevertheless outperforms any single event.
- Make performance data and rating information available to all large and small organizations' email gateways (and potentially other "competing" rating services) through standard query and response formats.

3.4 Required Changes for Outgoing Volume Email

Once senders and ESPs have been registered, Project Lumos proposes that enhancements the way registered email is generated and sent to allow receiving email gateways to authenticate the sender and (optionally) verify the authenticity of the content of their emails.

Enhancing the volume email sending process will include:

- Inclusion of electronic credentials of both the sender and ESP within the email headers.
- A security mechanism that will ensure no identity theft i.e. use of the credentials by any unknown party.
- A mechanism to ensure that the content of the emails may not be modified or that the email headers are not pre-pended to the body of other emails.
- A mechanism to ensure non-repudiation of the email and its content by the sender.
- A mechanism to ensure that the identity of sender and originating ESP may be confirmed at any point in the delivery chain.
- Appropriate permission-based email information such as unsubscribe and abuse reporting information in a standard fashion when appropriate.
- A mechanism that ensures reasonable overhead and processing cost for the encryption/decryption to enable volume use.

3.5 Recommended Changes for Incoming Volume Email Processing

Project Lumos assumes that email gateways will make certain changes to process the identity and reputation information for registered senders and ESPs. While Project Lumos ensures that an email gateway will be able to continue to receive email without implementing any changes, the benefits of secure sender identity can only be realized with some infrastructure upgrades.

Upgrading the volume email receiving process may include some or all the following:

- Reading electronic credentials of both the sender and ESP from the email headers.
- Decoding the secure (encrypted) signatures to ensure their authenticity.
- Checking the content of the message for authenticity.
- Look up performance ratings for authenticated sender and ESP.
- Use of performance rating and/or internal historical information in order to determine how to process the sender's email.
- Passing email through to end user mail client and indicating in the mail client that the message is from a verified source.

Monitor and aggregate information about sender and ESP performance in order to report back to the performance monitoring service.

3.6 Implementation and Operational Considerations

3.6.1 Implementation Requirements

Implementation of the Blueprint processes, standards, and physical components must meet a number of practical considerations. These include the following:

- All new standards introduced must be fully backwards compatible with existing email standards to allow inter-working with current servers and gateways, both for an extended transition period and for many servers that may not be upgraded.
- Implementation should allow for gradual transition to a fully cryptographically secure technology. Initial authentication may rely on an IP based solution providing the ID. It is the belief of Project Lumos that the email infrastructure must migrate to a fully secure implementation of digital signatures.
- The implementation must leverage existing technology infrastructure, such as digital signatures, certificates, encryption algorithms, etc. wherever possible to speed the transition and reduce the cost burden.
- All new data formats and protocols must be open standards based.
- Registries must provide a high level of performance so as not to impact email services.
- All data sources and communications must be compliant with the relevant national and international Privacy guidelines.
- The architecture and Registry implementation must be Anti-Trust Compliant, not precluding operation of competitive services for certification, performance monitoring and Registry functions.

3.6.2 Operational Requirements

Operation of the Registry or multiple Registries should be performed by trusted third parties. These third parties must be objective in their certification of senders and setting of policies and performance standards.

In addition to providing oversight and management of the certification and performance monitoring processes, Registry operators should provide access to a dispute resolution process for registered parties that do not feel their ratings accurately reflect the data or have had their certification revoked. The oversight function may imply a need to perform audits of registered senders and ESPs when required. The Trust Authority function could be implemented by third party entities such as TRUSTe or possibly firms such as Price Waterhouse Coopers (PWC) or Ernst & Young (E&Y).

4. Technical Description

4.1 Architecture Overview

As previously outlined, Project Lumos is a blueprint for an extension to the existing email infrastructure that eliminates spam by holding all volume senders accountable for the mail they send and their sending practices.

Figure 3 below provides an overview of the end state of the proposed systems architecture. Key components of the architecture include:

Registries – offering:

- Certification Services to validate the identity of senders and ESPs;
- Registration Services of certified senders and ESPs;
- Volume Email Standards: agreed to by the senders and ESPs during the registration process;
- Reputation Services: a repository of identity, performance data and rating information.

Enhanced Volume Email Delivery process encompassing:

- Enhancements to the email headers (new X-Headers) that provides Sender and ESP authentication information in the form of digital signatures, standardized, trusted unsubscribe links, abuse reporting information, etc.; and
- Receiving email gateway enhancements to utilize the modified email headers, validate the email source, check the performance rating of the sender and ESP, and determine the disposition of the incoming emails.

A Performance Measurement and Rating process – including:

- A mechanism for collecting sender and ESP performance data at the email gateway;
- A service that accepts all performance data, abuse complaints and unsubscribe requests; and
- A mechanism to calculate performance ratings for registered senders and ESPs.

Each of these three major aspects of the blueprint is described in detail in the following sections.

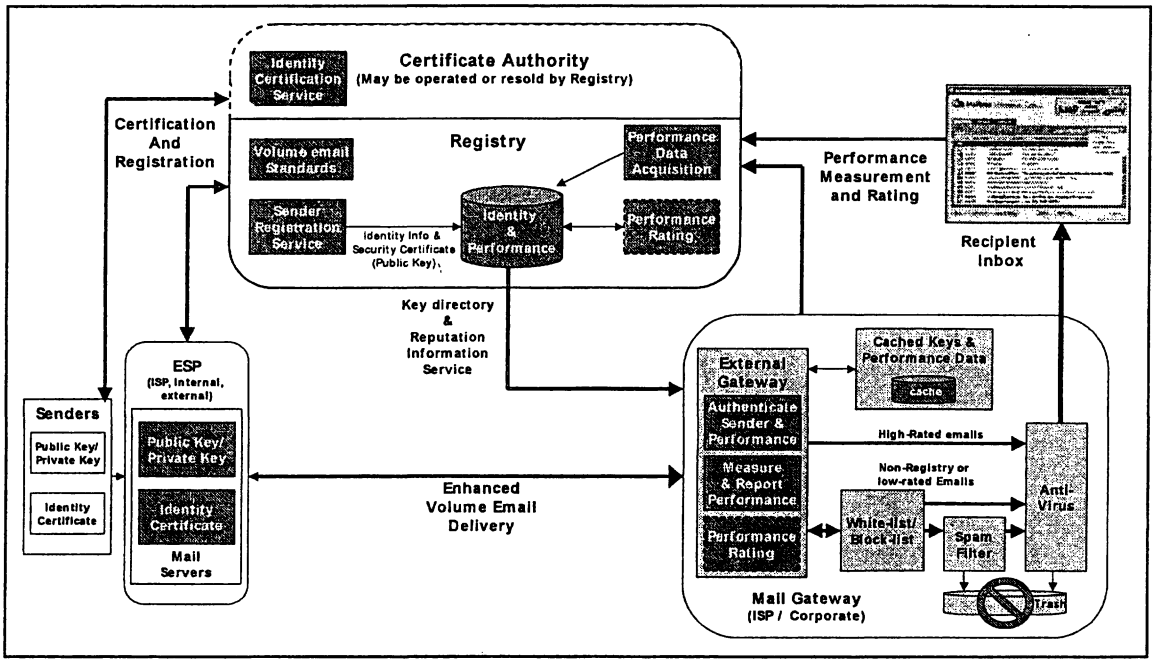


Fig. 3 – Systems Architecture

4.2 Certification and Registration Services

The Registry offers three primary services: the Certification service; the Registration service; and the Reputation service. These provide a verified and secure identity and associated electronic credentials to high volume senders and ESPs and, in turn, make the performance and identity information publicly available. A simple architectural view is shown in Fig. 4 and the functionality of the services explained in more detail below.

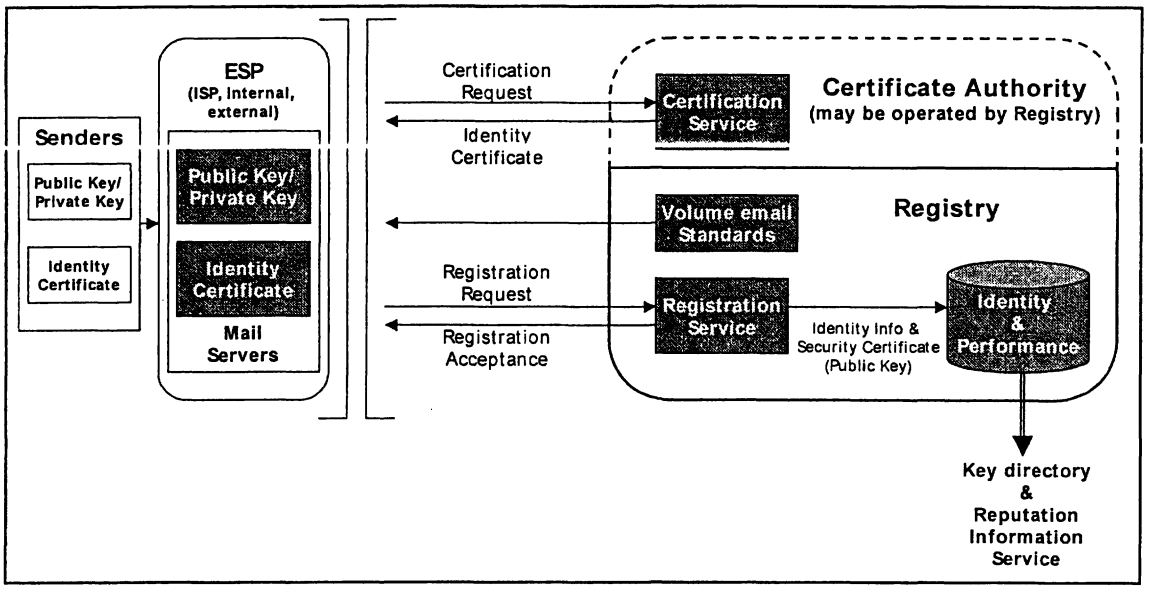


Fig. 4 – Primary Registry Services

4.2.1 Sender and ESP Certification Service

4.2.1.1 Certification Service Functions

The Certification Service can be operated by the Registry directly or can be operated by an independent Certificate Authority (CA). There can be multiple CA's and Registry operators.

The certification process starts with both high volume senders and ESPs applying for certification. They must provide sufficient information to clearly identify their true business or personal identity, and agree to adhere to the Terms of Certification as published by the Registry or Certification Authority. The operators of the CA or Registry use this information to verify the identity of the sender or ESP.

There will be multiple levels of Certification with higher levels of certification requiring a more in-depth authentication process. The highest levels of certification may be outside the reach of a small business or other small senders. Therefore, a Registry or CA may choose to issue less expensive, lower grade certifications based on a less rigorous identity check. Email gateways may choose to handle incoming mail differently based on the level of security of the associated certification. A lower grade certification may, for instance, become subject to sending rate limits by mail gateways. In combination with a good reputation, a lower level certification should nevertheless work as well as a high level certification. Reputations therefore ensure that even the cheap, quick certification process available to small businesses can lead to reliable email delivery as long as the business adheres to best practices.

While each Registry could establish its own certification classification scheme, and the certification process may be different for commercial and non-commercial senders of email, a consistent notation is proposed

for use by all certifying authorities. The proposed Classification scheme for Senders and ESPs is shown in Table 1 below.

Table 1 – Certified Sender Classification

Class Designation	Description	Authentication Mechanisms
A	- Large complex (global) organization - Commercial organizations or non-commercial such as not-for-profit organizations, government departments, political parties, or other NGOs - Multiple divisions require certification - Overall high volume of email with multiple points of origin	- Authenticated in 3 spheres: Government, Industry, Financial - Business registration number, Tax ID, Articles of Incorporation - Dunn &Bradstreet DUNs # - Registered Charity number - Credit letter or Credit card - Postal address validation
B	- Medium size business - Single point of certification - High volume of email with few points of origin	- Authenticated in 2 spheres: Government, Financial - Business registration number, Tax ID, or Registered Charity number - Credit letter or Credit card - Postal address validation
C	- Small, home business - Medium volume of email with single point of origin	- Authenticated in 1 sphere: Financial - Credit card, billing address verification
D	- Anonymous individual - Restricted to very low volume in the order of < 100 email/day	- Certification of Identity of Sender has not been performed - Used in combination with certified ESP/ISP

Internet Service Provider and Web mail providers will want to apply for Certification under the framework proposed above. Certifications tied to an ISP will support small business Senders (with Level C certification) as well as personal mail users (with Level D certification) who wish to remain anonymous. For instance, consumer oriented ISPs (e.g. Yahoo, Hotmail) may limit free mail to 100 messages per day and choose to require very little in terms of proof of identity. Alternatively, an ISP may require that all subscribers offer some form of proof of identity such that their usage can be tracked internally, but keep this confidential and not include it in the outbound message header. Likewise an ESP serving small businesses will require proof of ability to pay, but may have a relatively light weight verification mechanism and a corresponding rate limit – perhaps 10,000 a month at the lowest levels of certification.

Inexpensive, lightweight certifications are only viable if a service provider is motivated to monitor the performance of senders and use measures like rate limits as a means to enforce their performance and compliance with Volume Email Standards. Project Lumos introduces performance rating for ESPs as the primary solution for keeping ESPs (including ISPs) honest about their adherence to volume mail standards. Without rating the ESPs, the situation exists where either the accommodations for small senders amount to a big spam loophole, or where small senders are simply shut out. Neither is acceptable.

The Certification process should be based on existing mechanisms appropriate to the sphere and geography of operation of the Authority. Once the identity has been verified, the service will issue electronic credentials (signed certificates) to the applicants who will use these to validate the emails they send.

A Registry will be able to revoke the certification or change the electronic credentials of the senders and ESPs should their identities later prove to be invalid or the credentials be compromised.

4.2.1.2 Electronic Credentials

Robust security requirements suggest the use of Public Key Infrastructure (PKI) cryptography for authentication. Project Lumos is nevertheless not based on any specific mechanism or standard for securely representing identity and can be implemented based on a number of existing and emerging standards and technologies.

For initial implementation, certificates could, for instance, be based on existing X.509v3.0 certificate formats containing the identity, classification, certifying authority, and Public Key of each of the certified Senders and ESPs. In addition to HTTP and LDAP servers, it is envisioned that the DNS infrastructure might be used as the distribution mechanism for Public Keys, Volume Mail Standards, and other information.

Both sender and mail server certificates must be based on a lightweight, specialized email certificate format to minimize bandwidth consumption and encryption/decryption processing.

4.2.2 Volume Email Standards

The Project Lumos architectural blueprint is built on process, technology, and policy. Volume Email Standards are the policy component forming the foundation for an agreement between the email senders and ESPs, and receiving email gateways. Registries will specify mailing Standards that senders and ESPs agree to adhere to as part of the registration process. Gateways will measure particular criteria to assess performance against these Standards.

4.2.2.1 Baseline Criteria Example

Table 2 provides an example of a baseline set of high-volume email Standards.

Table 2 – Baseline High Volume Email Standards

Performance Criteria	Description	Example Baseline
Bounce Handling Standard – Hard	The way in which the originating mail server handles hard bounce responses from a receiving gateway.	Addresses not retried
Bounce Handling Standard – Soft	The way in which the originating mail server handles soft bounce responses with particular soft bounce codes from a receiving gateway	- Retry Frequency = hourly - Maximum retries = 5
Abuse Reporting Standards	A standardized abuse reporting process used by the Sender and/or ESP, specifying what, to whom and how to report abuse	All abuse reports routed to the Registry
Abuse Handling Standards	The Sender's commitment to action upon receiving an Abuse report from a Recipient (possibly via the recipient's ISP or IT department or the Sender's service provider).	Unsubscribe from all future mailings
Unsubscribe Standards	A standard format for unsubscribe information in emails that would make it possible to incorporate unsubscribe functions directly into the email clients. This would increase consumer confidence in the unsubscribe mechanism.	Standard format to be defined (see the following section)
Unsubscribe Handling Standards	The Sender's commitment to action upon receiving an Unsubscribe request from a Recipient (via a clickable link, a return email, referred email from the ISP or ESP, or verbal request). Unsubscribes will be tracked and logged.	-Unsubscribes routed via the Registry - Processed by ESP within 10 seconds

4.2.2.2 Mail Categorization

In addition to the set of volume email standards, Project Lumos proposes implementing voluntary email Categorization by senders and ESPs. This provides a more specific classification of email where each category receives its own performance rating, allowing improved decision making at the receiving email gateway, with a different response possible for each category. For example, a gateway may choose to accept all person-to-person email from a particular sender while not allowing bulk email delivery. It also offers the potential for less costly processing, allowing delivery of all mail of a particular category for a sender without further analysis.

The following Table proposes a set of email Category descriptions based primarily on the permission type attributed to the list used for the mailing.

Table 3 – Mail Categorization Proposal

Category	Type of Email	Comments
Category I – Personal	• Personal or business related person to person email • Consent is implicit.	Known individual Sender
Category II – Service	• Customer service transaction, communication, or notice such as legal or emergency notices, confirmation of receipt (e.g. of an order) or status • Consent is implicit.	Service or transaction related communications triggered by recipient action or legal/emergency requirement.
Category III – First Class Confirmed (Confirmed Opt-in)	• Newsletters, discussion boards, product announcements, sale announcements, etc. where the distribution list was creating using a confirmation email to the subscriber • Consent is explicit and confirmed.	High volume individually addressed email communications with explicit and confirmed consent from all recipients.
Category IV – First Class (Opt-in)	• Newsletters, discussion boards, product announcements, sale announcements, etc. where the distribution list was creating using subscriber opt-in. • Consent is explicit.	High volume individually addressed email communications with explicit consent from all recipients.
Category V – Bulk	• Mailing to existing customers, with a recent prior business relationship, without opt-in. Third party list rentals, opt-out with notice • Consent is implicit with opt-out	One to many mailings to legitimate email lists, without explicit recipient consent
Category VI – Unknown	• Unknown or un-trusted origin • Consent is unknown.	Unknown senders, unknown source of email addresses, etc.

4.2.3 Registration Service

Each Registry will publish their "Terms of Registration", their supported categories of certification, and the volume mailing standards (as per the proposed set described above) to which certified entities must adhere.

The Registration service is fairly simple. It will

- enforce acceptance of the Terms of Registration by senders and ESPs;
- accept the certified identity information and electronic credentials;

- establish the Identity information, an initial placeholder for performance data, and an initial 'null' performance rating in the Registry; and
- Support an appropriate "unsubscribe redirection link" that the sender will incorporate into outbound emails in order to track unsubscribes at the Registry (and any abuse of the unsubscribe process).

4.2.4 Reputation Information Service

The Reputation Service supported by Registries will provide identity information and performance data openly to anyone who requests it, keyed to the certified identity of the sender or ESP. Specific details of the performance data and performance rating information are discussed in Section 4.4 below.

The Blueprint recommends the development of a specifically formatted XML file that would be returned by all Registries in response to a query for the performance data and performance rating information.

4.2.5 Implementation Considerations

It is assumed that there may be multiple physical implementations of Registries operated by different third-party entities.

Furthermore, Certification, Registration, and Reputation services may be offered by the same or different organizations. A few potential scenarios are:

- Current "Certification Authorities" (CAs) extend their services to meet the Blueprint certification service while leaving operations of the Registries to other organizations.
- Organizations provide 'one-stop shopping' of Certification and Registry services.
- An organization offers one-stop shopping but the Certification is outsourced to a CA.
- An independent (set of) Reputation services may emerge providing performance and rating information about senders. These may be "bundled" by a registry or the registry may be implemented around the information/reputation service.

Other situations are possible as well. In any case, the Certification and other Registry Services must provide similar functionality.

In addition, some larger organizations such as corporations, ESP's, governments, or institutions might choose to self-certify and thereby effectively operate their own Registry. This would be permitted under the higher-level certification of an external CA just as it is possible for SSL Certificates and Personal Email certificates today. If a sender decides to self-certify, they will still need to enable certain performance data to be collected by an independent performance rating service.

4.3 Volume Mail Delivery Enhancements

Project Lumos requires that in order to make use of the secure identity and performance information certain functionality be implemented at both the ESP and receiving email gateway. Note that there are no fundamental protocol changes; the receiving mail gateways that choose not to implement the Lumos receive side enhancements can continue to use their existing infrastructure to receive mail that was sent with the Lumos enhancements.

Senders and ESPs must follow the Volume Mailing Standards in accordance with their registration agreement. Additionally senders and ESPs need to include email content authentication information as well as certain other information in the email headers.

Receiving email gateways must be able to decrypt and validate the digital signatures, access the performance data, and use this information to route the incoming email. These key enhancements to the volume mail delivery process are shown in the Figure 5 and described in more detail following.

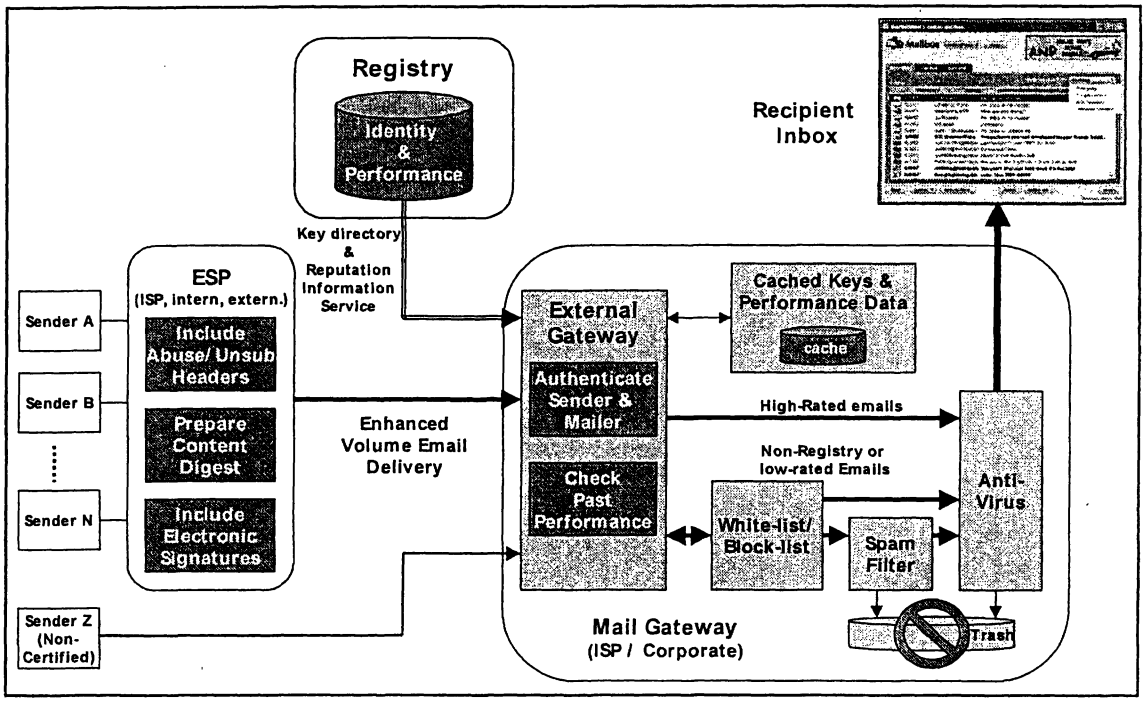


Fig. 5 – Enhanced Volume Email Delivery

4.3.1 Permission Email Information in SMTP Headers

Information such as unsubscribe and abuse return addresses and URLs is required for the proper operation of permission-based email. Project Lumos proposes these be included in the email headers in standard formats. Including these will, over time, allow email clients to help enforce potential legislation (e.g. by rejecting any email without a valid unsubscribe), provide a more trusted unsubscribe mechanism, and provide improved abuse reporting functions. It will also provide a simple, standard means for the gateways to ensure that the incoming email is meeting the volume email standards.

Permission email information added to the SMTP header will include:

X-Unsubscribe-To: The valid email address that can be used for unsubscribing.

X-Unsubscribe-URL: This is a complete URL used for automated unsubscribe. Sending a request to

this URL should unsubscribe the recipient from this list.

X-Abuse-To: Abuse reporting email address to which ISP's or other Gateway operators should forward abuse reports.

X-Abuse-URL: This is a complete URL used for automated abuse reporting. Sending a request to this URL should report abuse for this recipient and for this campaign.

X-Abuse-Copy: Abuse reporting email address to which the ISP or other Gateway operator should forward a copy of all abuse reports. This address will normally be with the registry and used to monitor the performance of Senders and ESPs

X-Message-Cat: Message Categorization type definition as per the Volume Email Standards section.

X-Campaign-ID: An alphanumeric string which uniquely identifies the specific volume email contents. It should be unique to the ESP sending the emails.

Each of these additional header fields will use the X-Header extension standard and are therefore optional in individual person-to-person messages and messages sent to small distribution lists. An X-Header based solution provides a simple transition path and minimizes the overall impact on the email infrastructure. In time, receiving email gateways will refuse to accept high volume mailings, or mailings from specific volume ESPs, without these headers and low-volume Senders such as individuals will use the anonymous categorization sending from a known (and well rated) ESP.

4.3.2 Authentication Information in SMTP Headers

Project Lumos stipulates that electronic signatures of both the sender and ESP be included in SMTP headers as secure proof of identity. In addition to providing proof of identity, signing the email will ensure that the email body is not changed, or that valid email headers are not duplicated and placed on invalid email bodies. The sending Mail Server will execute a message digest function, performing an inexpensive hash on the message (e.g. using the standard SHA-1 Secure Hash Algorithm), encrypt the message digest using the sender's and ESP's private keys (e.g. using the DSS Digital Signature Standard), and include both signatures in the email headers.

The X-header format will also be used for inclusion of the authentication information allowing implementation with no changes or enhancements to standards, servers, or gateways:

X-Sender-ID: The certified ID issued to a Sender by the CA. Used to identify the Sender and access their public key. This may take the form of the distinguished name of the certificate issuer followed by the certificate serial number

X-Sender-Sig: The digital signature of the Sender.

X-Sender-Registry-URL: The URL of the Registry containing the Sender information.

X-ESP-ID: The certified ID issued to an ESP by the CA. Used to identify the ESP and access their public key.

X-ESP-Sig: The digital signature of the ESP.

X-ESP-Registry-URL: The URL of the Registry containing the ESP information.

X-Message-Dig: The message digest hash result.

With the Registry URL and the ID, receiving email gateways will be able to acquire the published public keys from the registry and decrypt the digital signature of both the ESP and the sender to validate their identities and the content of the email.

Once these have been more widely adopted, the proposed X-Header extensions should be considered under the IETF's RFC process for standardization and permanent adoption into SMTP.

4.3.3 Receiving Email Gateways

Receiving email gateways will implement their own delivery policies based on their ability to identify a registered sender and ESP, and access their reputation – the historical performance record of this sender.

4.3.3.1 Authentication at the Receiving Email Gateway

An email gateway will perform the following functions and make a decision based on its own delivery policy for the disposition of incoming email. For performance reasons, email gateways are likely to utilize a combination of caching and other performance optimizations to reject clearly non-compliant messages early in the process.

Authenticate the ESP – The gateway will use the originating ESP's identification contained in the email header to look up the ESP's public key in the Registry. It will then decrypt the ESP's digital signature in the header comparing against the message digest to validate the identity of the ESP.

Authenticate the Sender – The gateway will use the sender's identification contained in the email header to look up the sender's public key in the Registry. It will decrypt the digital signature in the header in a similar fashion to validate the identity of sender.

Check Performance Ratings – When it requests the public keys, the gateway will also receive the latest performance ratings for each of the sender and originating ESP from the Registry. It will update any local cache and classify the incoming messages in accordance with their performance rating.

Authenticate the email content – The gateway may further validate the email contents by recalculating the message digest on the body of the email, and comparing the results against the value in the header. If they are identical, there is a high certainty that the message has not been tampered with.

Message Disposition – Once classified, the gateway will route the email message, either sending it to the recipients inbox, routing it to the bulk mail folder, or rejecting outright, based on the gateway's locally set criteria.

Once this process has been completed for the first incoming message of an email campaign, all other messages may be treated in a similar fashion. Moreover, if the ESP has proven to not follow the established standards, or if they are not registered, the message stream may be rejected without further processing.

4.3.3.2 Caching and Performance Optimizations (Recommended)

The most cost effective place for an Email Gateway to reject an incoming message is at the point of connection from the sending mail server. The second most cost effective point of rejection is after reading the headers, but without analyzing the entire message body. These performance optimizations can be achieved with a combination of IP white listing and public key caching.

Registries will publish the IP addresses of all registered mail servers. Email gateways can use their existing white list technology to reject all connections from mail servers that are not registered at a known registry. White list information, much like block list information, can be cached locally or looked up at a DNS server maintained by each registry.

For performance reasons, receiving gateways should cache the sender and ESP information, including their public keys and latest performance rating. This would eliminate the step of requiring a query to one or more Registries each time a new mail stream was initiated and reduce processing and bandwidth resources at the

gateway. Aging criteria on the cache will be required to ensure latest performance rating is available as well to validate that the public keys have not been revoked or changed.

Numerous other optimizations are possible with volume messages. For example, an email gateway might choose to completely validate an incoming message with a unique campaign id, but skip some steps on subsequent messages over the same connection with the same campaign ID, sender, and ESP.

4.4 Performance Measurement and Rating

The primary goal of performance measurement and rating is to establish the 'reputation' or track record (good or bad) of senders and ESPs over time. Project Lumos proposes the establishment of a Reputation Service that is focused on collecting, consolidating, and disseminating objective, network wide information about senders and ESPs such that recipients and gateways can use this information to determine how to treat incoming mail. Since the performance rating would be tied to the secure identity, changing identities of the sender will cause the loss of their established performance record making it difficult to churn identities. Senders or ESPs with no proven track record (i.e. with no reputation) will be treated cautiously by the receiving gateways.

It is not sufficient to rate only the mail sender. The sender's agency (ESP), if any, must also be rated. This provides additional necessary controls in the system and is critical to the enforcement mechanism:

- Motivating ESPs to police their clients;
- Providing a reputation surrogate for new senders who have not yet established a reputation;
- Providing a means of aggregating small senders such that they can be held accountable for their abuse complaints.

The performance ratings for senders and ESPs are based on the historical performance information measured and provided by a variety of receiving gateways and through redirects and referrals of un subscribes and abuse complaints from the recipients. The Performance Data Acquisition service of the Registry captures and consolidates the data, while the Performance Rating service executes an algorithm that determines the ratings. This is depicted in Fig. 6 below with details described in the following sections.

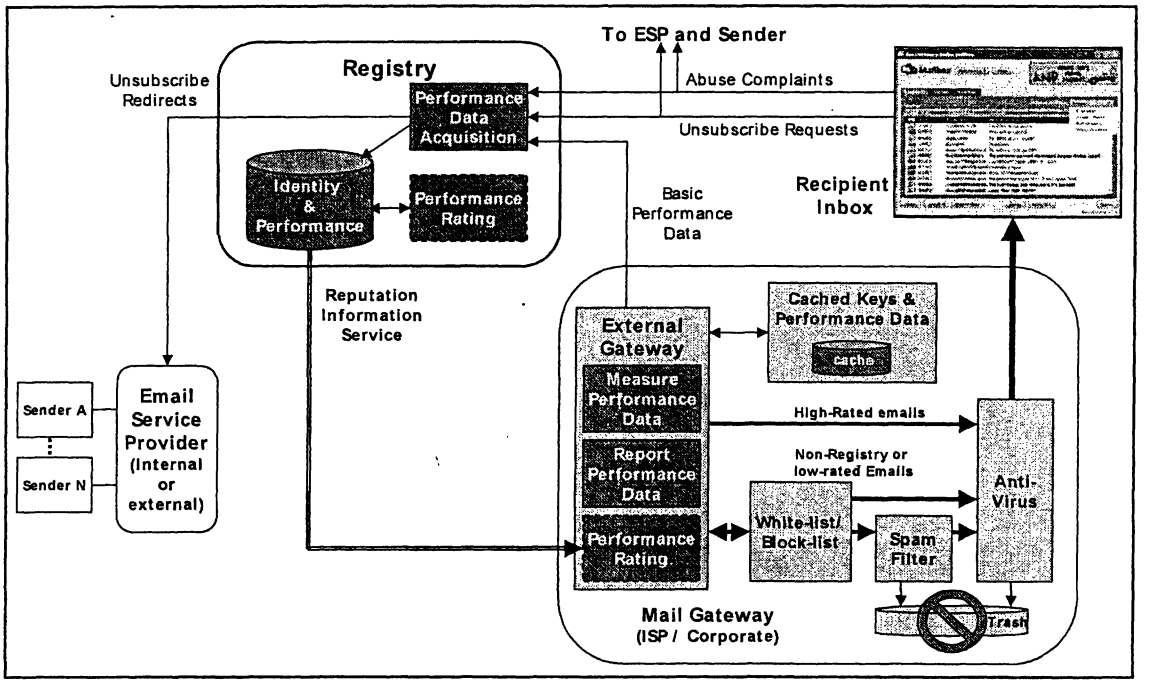


Fig. 6 – Performance Measurement and Rating

The performance rating algorithm will be developed by a Rating Service, which in most cases will be operated by a Registry. However, the base performance data will be made available in order for receiving gateways, existing anti-spam products, or external performance rating agencies (similar to the operation of credit agencies) to implement their own performance rating schemes.

4.4.1 Performance Data

Performance data is collected and associated with Campaign ID, Sender ID, and ESP ID providing unique identification and summarization capabilities. Sender ID and ESP ID are defined through the certification process while the Campaign ID provides a convenient way for Senders or their agents to track their individual mailings and identify potential performance and compliance related problems. Project Lumos proposes collecting the following Performance data as the basis of the performance rating.

Table 4 – Performance Data Measurements

Performance Criteria	Description
Message Volume	The total volume of email sent in a particular campaign as well as the aggregate volume from each Sender and ESP. Volume is also tracked for each sender and ESP by category of email, using the categorizations described earlier.
Hard Bounce Count	The count of hard bounces, messages without a valid, known email address. This will be a good indicator of the quality of the email address lists used.
Duplicate Unsubscribe Count	The count of duplicate unsubscribe requests by the same recipient, on the same list from separate campaigns. A duplicate unsubscribe is an indication that the sender is not handling unsubscribe requests properly.
Abuse Complaint Count	The count of the number of unique recipients who report a particular campaign as spam. The abuse complaint rate will be a key factor in the performance rating. While some complaints may be unjustified, the majority of abuse complaints indicate that the sending of the email to this recipient was inappropriate.
Repeat Abuse Complaints	Repeat offenses of spam complaints are indicative that the ESP or sender is not taking appropriate action in response to complaints.
Receiving Gateway Abuse Complaints	This is a count of the number of complaints from Gateway administrators who complaint about the ESP's volume emailing technical practices (such as abusing bounce retry guidelines, receive rate too high, etc.).
Accuracy of email categorization	A true/false value indicating if the message type has been categorized correctly (as per the Volume Email Standards). Since the sender or ESP will set the category, an assessment of whether the email was categorized correctly will provide a means of policing the accuracy.
Recipient Rating	An indicator of Recipient's subjective view of the value and quality of the received email. This may be used in future implementations of performance using a "Rate this Email" feedback function in the email client.

Some of this data defined above will be used in initial Rating formulas such as the example proposed below, while some data (such as the Recipient Rating) may be used later as industry experience grows and rating formulas increase in sophistication.

4.4.2 Performance Data Acquisition Service

The Performance Data Acquisition service performs three significant functions. It collects and consolidates basic performance data as measured by the gateways. It captures abuse complaints directly from recipients. And finally, it captures unsubscribe requests in order to assess the senders' compliance to unsubscribe handling standards.

Registries should be prepared to accept partial data. For example, they should accept abuse complaints and unsubscribes even if the receiving gateways are not yet prepared to provide the hard bounce count.

4.4.2.1 Basic Performance Data

The Registries will implement a Data Acquisition Service to capture performance data from a potentially very large number of receiving gateways, and consolidate, organize and store the data for the reported sender or ESP. The information to be captured is based on the Volume Email Standards and the Performance Data Measurements described in Table 4.

Receiving email Gateways will be expected to play a direct role in the development of the performance ratings. They will be responsible for measurement and forwarding of performance information to the Registry(s). With each new incoming volume email campaign, they collect and report on the data.

Standard performance data reporting syntax and semantics will be required to enable the Performance Data Acquisition Service. Project Lumos recommends the implementation of the reporting function as follows:

- The data must include Campaign ID, Sender ID, and originating ESP ID thereby providing unique, campaign level tracking and scoring.
- The data must be reported to the Registry for the sender and that of the ESP, or only one if available.
- An initial report on a newly received campaign should be constructed and submitted within no more than 24 hours of the receipt of the first emails in the campaign.
- The time period covered by the report should be included in the submission.
- The reporting mechanism would allow for 'updates' of the data, possibly on a daily basis, as more recipients open the emails and potentially take action such as unsubscribing or reporting abuse.
- The reporting format would include an attribute to distinguish an initial report for a newly received campaign to that of an update for a previously reported campaign.
- An earlier submission or more frequent submissions would be acceptable
- An XML document format should be standardized for submission of the performance data

Prior to the development of standard report document formats, Registries should initially offer at least two alternatives for submission: a secure web form submissions, and a text file submission on a specified tag-value format.

4.4.2.2 Capturing Abuse Complaints

Project Lumos proposes the development of a standardized Abuse Reporting Process starting with the abuse reporting addresses embedded in the headers of the emails. As part of this process, in addition to the abuse reports being sent to the sender and ESP of the volume email, they will be copied to the appropriate Registries.

The Registries will use the Sender ID, ESP ID, and Campaign ID embedded in the headers to properly categorize the abuse report. Moreover, they will check if the recipient has reported a prior abuse from this sender. 'Repeat Abuse Reports' will be particularly damaging to the sender's performance rating.

4.4.2.3 Processing Unsubscribes

Spammers often abuse the unsubscribe process by including fake unsubscribe links in spam email. Establishing a trusted unsubscribe mechanism is accomplished in Project Lumos by associating the secure identity of the sender with the oversight of unsubscribe processing. In order to determine that the proper actions are being taken in response to unsubscribe requests from the recipients, the Registry must be made aware of all of these requests. Project Lumos proposes that the unsubscribe mechanism employ a web redirection process to accomplish this.

The 'unsubscribe redirection link' format must be accepted as part of the registration terms. The ESPs will use this format when constructing a complete link by concatenating the redirection URL, the sender and ESP IDs, and other campaign specific information generated by the ESP.

These complete links will then be built into the: i) header of the email where it can be interpreted by the email client; and ii) body of the email as is current practice today. In the short term, the link in the body of the email will be used for unsubscribing. Eventually it may be replaced by email client software functionality.

4.4.3 Performance Rating

The Performance rating formula will calculate an objective value representing the sender's and ESP's reputations from some of the measured data over time.

Rating = f (Hard Bounce Count, Repeat Unsubscribes, Abuse reports, Volume, Time)

The Blueprint proposes an initial, simplified rating algorithm as a working example. It is expected that the Registries or other performance monitoring agencies will develop their own formulas, and that these will become more sophisticated as the industry gains more experience with the available data. As there is currently no reliable data on which to build a score, it is likely that any initial formula can and will be improved.

4.4.3.1 Proposed Rating Scale

It is proposed that the performance ratings be scored on a simple 0-100 point numerical scale, where 100 is perfect and a null or empty score corresponds to no rating.

All reputation scores are built from publicly available data stored at the Registry. Any organization could query this data and devise its own scoring system. The scoring from 0 to100 is specified to enforce a standard in score semantics.

4.4.3.2 A Simple Rating Formula

Like a financial credit rating, the performance rating ages over time. The example formula uses 100 days as the time window so that a quarterly sender can maintain their reputation. The score for the current 100 days is doubled and added to the score for the previous 100 days and then the total divided by 3. This gives a weighted average for the last 200 days.

The total Performance Rating is calculated as

Rating = Minimum[0 , ((2 * CurrentScore) + previous 100 day score) / 3]

While the basic measure of the score for the most recent period is:

CurrentScore = 100 – (AbuseRate*1000) – BounceRate – (DupUnsubRate*10000)

Where:

AbuseRate = 100-day running average of the abuse rate where the absolute number of reports exceeds X/100,000 where X is known number. The 100-day running average ensures that a quarterly mailer can maintain their reputation.
Furthermore, due to current abuse reporting mechanisms, a minimum threshold of abuse complaints must be exceeded to ensure some level of statistically meaningful accuracy for very small senders. For illustration purposes, this threshold is set at 5 for a 100-day period.

BounceRate = 100-day running average of the bounce rate.

DupUnsubRate = 100-day running average of the duplicate unsubscribe rate. Note that this is a duplicate unsubscribe on the same list from separate mailings; mailers are not penalized when someone hits "unsubscribe" multiple times on the same mailing.

To use an example, if a relatively large sender, has the following campaigns, all sent to his entire list:

Campaign Name	Date	Send Count	Abuse Count	Bounce Count	Duplicate Unsubscribe
New Store Opening	May 10th	400,000	1	80,000	0
A New Look	June 1st	425,000	25	200	0
Our Renovated Web Site	July 15th	500,000	2	400	0

The 100 day send volume is: Volume = 400,000 + 425,000 + 500,000 = 1,325,000
The 100 day abuse rate is: AbuseRate = (28/1,325,000) * 100 = 0.002%
The 100 day bounce rate is: BounceRate = (80,600/1,325,000) * 100 = 6.0%

Giving a current score of: CurrentScore = 100 – (0.002*1000) – 6 – 0 = 92

Note that failure to remove bounced addresses from the list would presumably give:
Volume = 400,000 + (425,000 + 80,000) + (500,000 + 80,200) = 1,485,200
BounceRate = ((80,000 + 80,200 + 80,600)/1,485,200)*100 = 16
Resulting in a total current score of:
CurrentScore = 100 – (.002*1000) – 16 = 82

In practice, however, the score would most likely be lower as senders who fail to remove bounces generally also have poor unsubscribe and abuse handling practices leading to penalties on those scores as well.

Looking at a second example of a small sender, with a somewhat seasonal business:

Campaign Name	Date	Send Count	Abuse Count	Bounce Count	Duplicate Unsubscribe
Winter Newsletter	January 15th	500	0	50	0
Spring Newsletter	April 11th	2,500	2	350	0
Father's Day	June 6th	4,000	2	325	0

Here the total abuse count in the period is less than 5, so it is ignored. Note that one more mailing with 2 abuse complaints would put this mailer over the abuse count minimum and the rate would be computed as part of their score.

The 100 day send volume is: Volume = 500 + 2,500 + 4,000 = 7,000
The 100 day abuse rate is: AbuseRate = 0 (did not exceed minimum threshold of 5)
The 100 day bounce rate is: BounceRate = (725/7,000) * 100 = 10.3%

Giving a current score of: CurrentScore = 100 – (0 * 1000) – 10.3 = 89.7

When performing the calculation for an ESP, the abuse and bounce rates consider the total number of abuse complaints, bounces, and email volume for all of the senders using that ESP. Thus the ESP score is not a simple average of its users' scores, but is weighted such that higher volume senders have a larger impact on the rating.

Calculating the score for an ESP that provided service to both of the above senders in this example:

The 100 day send volume is: Volume = 1,325,000 + 7000 = 1,332,000
The 100 day abuse rate is: AbuseRate = ((28 + 4)/1,332,000) * 100 = 0.0024%
The 100 day bounce rate is: BounceRate = (81,325/1,332,000) * 100 = 6.1%

Giving the ESP a current score of: CurrentScore = 100 – (0.0024*1000) – 6.1 – 0 = 91.5

With the total Performance Rating calculated as

Rating = Minimum[0 , ((2 * CurrentScore) + previous 100 day score) / 3]

A mailer with a current score of 90 and a previous score of 60 would have a Rating = ((2*90) + 60)/3 = 80.

Conversely, if performance had degraded and the current score was 60 with a previous score of 90, then the result would be: Rating = ((2*60) + 90)/3 = 70.

Improved performance is rewarded while degraded performance is punished. While the scoring formula could conceivably result in a negative number (for a very high abuse or duplicate unsubscribe rate), the Minimum performance rating is set to zero.

4.4.3.3 Other Rating Formulas and Future Improvements

The previous is a simplistic example to show how several of the performance measurement factors can be incorporated into the calculation – abuse and bounce rates are widely understood concepts, even if not currently accurately reported. As the industry gains experience with the data, better formulas will emerge.

It is easy to imagine an improved formula that ages out more gracefully over a longer period of time. For example, averaging over a year but assigning heavier weights to more recent time periods. Future improvements may also include adding data to the performance scoring, such as a scheme for reporting and tracking category violations separately from general abuse complaints or a recipient rating system. These have not been included here in order to simplify the initial deployment proposal.

5. Phased Implementation

Implementation of Project Lumos will not be a rapid cutover but require a phased transition over 18-24 months. Basic sender and server certification and secure identity will be implemented first. Basic performance tracking will be implemented in the near term, while more detailed aspects (such as sender and ESP rating) will require additional time. The following phased approach appears to be aggressive yet realistic.

Phase 1 – implemented in 1 to 6 months

- All commercial high volume ESPs will publish their mail server IP addresses, and provide the X-Unsubscribe-To, X-Unsubscribe-URL, X-Abuse-To, X-Abuse-URL, X-Abuse-copy, X-Message-Cat, and X-Campaign-ID headers.

Phase 2 – implemented in 6-12 months

- All commercial high volume ESPs will provide digital signatures and all header information described above in Section 4.3. Servers must encrypt headers and provide a message digest. Some senders may not yet have a public/private key pair.
- All commercial ESPs and Senders will conform to at the proposed baseline Volume Email Standards as a minimum.
- Lists of high volume commercial ESPs (containing IP addresses, Domain Names, Certified IDs, and their Public Keys) will be published by NAI and other industry groups. This will include Senders where digital certificates are available.
- Anti-spam filters may be tightened up for volume ESPs and Senders that have not been registered.

Phase 3 – implemented within 18 months

- Will see the first Email trust Registries beginning operation. They will expand the certification process and begin the issuing email specific certificates.
- Other volume Senders will obtain the new certificates and commercial Senders and ESPs will replace their certificates.
- At this time it is expected that all volume email will use encrypted headers and anti-spam filtering settings may be tightened further. Current anti-spam software may begin to evolve into email performance measurement software.
- Basic performance monitoring and reporting begins at the Receiving Email Gateways and the measurement information is submitted to the Registries.

Phase 4 – implemented in about 18–24 months

- Registries, with their certification and performance rating services, are in full operation. All volume email will be subject to authentication, performance ratings checks and performance monitoring,

By the end of Phase 4, email sent from unknown, unregistered Senders and/or ESPs will be unlikely to get through to recipients' inboxes or will be rate limited disallowing any high-volume delivery without secure identity.

6. Conclusion

6.1 Summary

By holding the sender and the Email Service Provider accountable for their sending practices and the content of their volume email, the email spam problem may be virtually eliminated. The solution described in detail in this document proposes a Registry-based architecture that implements this accountability.

A Certification Service will ensure that each high volume email sender and ESP verify their identity and commit to a set of standards for sending volume email. A secure method, built around a lightweight PKI implementation, for including the sender identity, ESP identity, and a message digest in the email headers will allow the receiving email gateways to validate the source and content of the emails. And finally, the reputations of registered senders and ESPs will be established through continuous measurement of their performance in compliance with accepted volume mail standards. Finally, an objective rating will be calculated for each sender and ESP based on their historical performance.

With secure identities, knowledge of the best practice standards, and performance ratings available from a Registry, receiving email gateways will be equipped to make informed decisions about processing incoming email. Based on the sender's reputation they will have the option of passing the mail freely, subjecting it to a series of anti-spam filters, routing mail to a bulk mail folder, or blocking the email altogether.

Project Lumos presents an open, decentralized architectural model based on evolving inter-operable standards for information sharing. A phased approach to implementation is expected. Implementation will be facilitated through a requirement for backwards compatibility with existing email technologies providing inter-operability for organizations that choose not to implement an actual solution.

6.2 Outstanding Issues

There remain a few key outstanding issues that must be addressed prior to the implementation.

1. Who will own and operate the Registries, and under what detailed business model?
2. Is a separate Organization required to oversee the operations of the Registries and provide a dispute resolution mechanism?
3. How does Project Lumos work with the standards bodies such as the IETF to create the standards necessary to ensure effective definition and communication of the identity and performance data?

Discussion within and external to the NAI ESPC has begun to resolve these issues.

6.3 Next Steps

There are several key activities, both short and longer term, required in the implementation of Project Lumos. Short-term next steps, to be addressed within the next couple of months, include:

- Industry providing critical analysis and feedback on the blueprint contained in this white paper.
- Finalizing the baseline Volume Email Standards outlined above.
- Finalizing an initial set of performance data collection and reporting protocols.
- Agreement on an initial Certificate format, leveraging existing technology as much as possible, for Phase 1 implementation.

In the 2-6 month term, next steps required include:

- Preparation and submission of draft standards for extension of the email headers including both the authentication information and permission email information.
- Development of XML document format standards for the submission of performance reporting information and access to performance rating information.

- Development and submission of a draft standard for a lightweight PKI certificate for email.
- Begin discussions regarding Certification and Registry operation with interested industry partners.

With these issues addressed, implementation of a trial Registry may be achieved within 3-9 months.

Appendices

FAQs

Q. How does Project Lumos stop SPAM?
A. By holding the owner of the mail server and the mail originator responsible for what they send and how they send it. Recipients' actions will directly impact performance ratings and their mail gateways won't accept poorly rated mail.

Q. How is a Spammer shut off?
A. A spammer that attempts to subvert the system or violate the registration agreement may be shut off by having their certification pulled. This will be the responsibility of the Registry. But because of the performance rating system, a great deal of the more mundane enforcement will occur as a natural result of the sender's and ESP's desire to maintain their brands and the viability of their businesses. Economic incentives are powerful. ESPs will not permit errant senders to degrade their performance rating, and Senders with legitimate businesses will, like all legitimate business owners everywhere, guard their reputations.

Q. Privacy – how do those who need to remain anonymous get their mail through?
A. By spring 2004 they will need to use a service that supports anonymity. Presumably non-commercial emailbox providers will continue to provide this service. Non-commercial emailbox servers may choose to implement rate limiters to protect their performance ratings.

Q. What happens to the small non-commercial ESP?
A. By spring 2004 they will need to obtain an "SSL-like" certificate, but nothing except deliverability concerns forces them to do this.

Q. Can a non-commercial originator use a commercial sender?
A. Yes. The originator's credentials do not need to come from the same authority as the mail sender's. This may be common in that organizations such as UNICEF may choose to use a commercial ESP.

Q. What about free emailbox providers?
A. In the simplest scenario, they may choose to rate limit and classify their users as "anonymous". Others may offer Sender certification services. Providers that neither control sending through their mail server nor require authentication will tend towards poor performance ratings.

Acknowledgements and Contact Information

To provide comment or feedback on the Project Lumos white paper, please contact:

J. Trevor Hughes
Executive Director – Network Advertising Initiative
Email: thughes@networkadvertising.org

Hans Peter Brøndmo
Project Lumos Technical Working Group Chair
SVP – Strategy and Corporate Development, Digital Impact
Email: brondmo@digitalimpact.com

Margaret Olson
Project Lumos Technical Working Group Co-Chair
CTO and VP-Architecture, Roving Software
Email: molson@roving.com

Paul Boissonneault
Project Lumos White Paper Principal Author
Email: pboissonneault@sympatico.ca

We would like to acknowledge the contributions of the many people who have been either involved in Project Lumos and/or provided valuable input into development of this white paper.

NAI ESPC Technical Working Group:

Derryl Rasquinha	GotMarketing
Brooks Dobbs	DoubleClick
Rob Raisch	IMN
Peter Mesnik	IMN

NAI ESPC Communications working group:

Leslie Price	Experian; Chair, NAI Communications Committee
Anna Zornosa	Topica; Former Chair, NAI Communications Committee
Kathleen Bagley	Blast! PR
Gail Goodman	Roving Software
Ashlen Cherry	Digital Impact
Dave Fowler	@Once
Andrew Marchese	Digital Connexxions
Lou Weiss	Blue Dolphin

NAI ESPC Legislative Working Group:

Ken Hirschman	Digital Impact	Ashlen Cherry	Digital Impact
Tony Hadley	Experian	Quinn Jalli	MindShare Design
Bennie Smith	DoubleClick	Elise Berkower	Doubleclick

External contributors:

Harry Katz	Microsoft	Dave Brussin	ePrivacy Group
Kevin Dorr	Microsoft	Vince Schiavone	ePrivacy Group
Brian Arborgast	Microsoft	Fran Maier	TRUSTe
Nicholas Popp	Verisign	Chuck Curran	AOL
Jeff Burstein	Verisign	Joe Barrett	AOL
Enrique Salem	Brightmail	Carl Hutzler	AOL
Ken Schneider	Brightmail	Lisa Pollock	Yahoo!

Other Anti-spam Initiatives

There are a number of other anti-spam initiatives underway. They may be categorized into public organization or private consortium initiatives, server-based anti-spam solutions, and client-based (desktop or laptop) anti-spam solutions. Examples of each of these are described below.

Public or Private Consortium Initiatives

IETF/IRTF Anti-Spam Research Group (ASRG)

The Internet Engineering Task Force (IETF) supports a number of small research groups within its Research Task Force (IRTF) working on topics related to Internet Protocols, applications, architecture and technology. Formed in Feb. 2003, the charter (available at http://www.irtf.org/charters/asrg.html) of the ASRG describes that:

> "The purpose of the ASRG is to understand the problem [of unwanted email messages] and collectively propose and evaluate solutions to the problem. While some techniques focus on local text classification approaches, many traditional and evolving techniques include approaches that involve new network architectures or changes to the existing applications and protocols.
>
> ASRG will investigate the spam problem as a large-scale network problem. The ASRG will begin its work by developing a taxonomy of the problem and the proposed solutions. This taxonomy should involve casting the spam problem into different perspectives, such as examining the similarities between spam and denial-of-service; spam and intrusion detection/prevention; and spam and authentication, authorization, and accounting.
>
> ASRG will consider the issues of deployment for proposed solutions, emphasizing the investigation of methods that have a realistic chance of wide-scale deployment.
>
> The work of the ASRG will also include investigating techniques to evaluate the usefulness and cost of proposed solutions. Usefulness is described by the effectiveness, accuracy, and incentive structure of the system. The cost of the system refers to the burden imposed on users and operators of the communications system. These costs include any changes to the normal use of the system or actual changes in the monetary costs of using the system."

To date the ASRG has produced draft documents on Requirements and Technical Considerations (such as approaches and evaluation criteria for adoption) for spam control.

TRUSTe

TRUSTe is an independent, nonprofit organization that offers a number of privacy certification and "trusted seal" programs for web sites and email. TRUSTe is sponsored by a coalition of web publishers, software companies and service providers. Organizations may display the Trust seal on their web site and/or within their email if they agree to a number of information privacy practices and display a clear privacy policy. An oversight and complain handling process supplement the seal programs.

TRUSTe also provides program certification, oversight, and dispute resolution services for Ironport's Bonded Sender program. TRUSTe monitors complaint rates, audit compliance with program standards for senders, and resolves disputes related to the legitimacy of complaints.

Trusted Email Open Standard

The ePrivacy Group released a white paper presenting the "Trusted Email Open Standard" (TEOS) on April 30, 2003. TEOS proposed an approach to the fighting spam that includes three key aspects:

- creating a trusted identity for email senders based on secure, lightweight electronic signatures in email headers, optimized with DNS-based systems for flexibility and ease of implementation.
- providing a standard structure for including trusted assertions about the content and sender/recipient relationship in the headers of individual messages. ISPs and email recipients could use these assertions to manage their email.
- Allowing the inclusion of an optional, visible 'trust seal' in the email for high volume senders along with standard practices, an oversight board and dispute resolution mechanism.

The ePrivacy Group is also offering royalty-free email Send and Receive engines incorporating the first two of the aspects above. The white paper is available at http://www.eprivacygroup.com/teos.

SenderBase

SenderBase is a free information service offered by IronPort Systems Inc. to email administrators to help them distinguish between legitimate sources of email (by IP address) from spam. SenderBase provides a global measurement of email volume, groups related sources of email, and is building a profile on individual senders. The information is available via a web interface at www.senderbase.org.

AOL, Microsoft, Yahoo!, Earthlink Anti-Spam Initiative

Microsoft, AOL and Yahoo, all large email service providers, announced in April 2003 that they will work together and lead a broader online industry effort to address spam. The group will initiate an open dialogue that will include organizations across the industry to drive technical standards and industry guidelines that can be adopted regardless of platform. Their initiative will focus on 4 main areas:

- Protecting consumers from receiving spam through the prevention of deceptive techniques in email headers that conceal the identity of the email sender and source of the email by leveraging existing directories of Internet addresses such as the Domain Name System, and inhibit email from systems determined to be open to unauthorized use.
- Preventing the use of their email services to send spam through elimination of fraudulent email accounts and exchanging consumer complaints and sender information to ensure a spammer does not just move to another ESP.
- Develop a set of commercial email standards, technical approaches, policies and best practices for businesses to communicate with consumers through email.
- Working with law enforcement agencies to augment their efforts against spammers who rely on fraudulent means of transmission.

These joint initiatives complement individual efforts by each of the three providers to enhance email-filtering capabilities, simplify abuse complaint reporting, and pursue legal action against spammers.

SpamAssassin

SpamAssassin is an open source anti-spam product that uses a variety of techniques for filtering incoming email. It uses a rule base to process both email headers and the body text, accesses a number of blacklists such as ordb.org and mail-abuse.org, and also accessing a database of previously reported spam to filter like messages.

SpamAssassin may be deployed at either mail servers or mail clients.

Server-Based Solutions

Brightmail

Brightmail is a private company offering anti-spam and anti-virus filtering software to ISPs, large enterprises, governments, and other organizations. Brightmail uses a large set of email addresses to collect illegitimate spam email and uses these to establish a set of source address, header rules, and content rules to identify spam. These "signature files' and blacklist entries are subsequently loaded into production installations of the Brightmail product at receiving email gateways allowing administrators to identify and delete, modify, or forward the spam email.

Brightmail's client base consists of a number of large ISPs and telecom service providers.

IronPort Systems Inc.

Ironport offers a family of email infrastructure Messaging Gateway Appliances. Their "A-Series" products are optimized for high volume commercial email delivery systems, while the "C-Series" are built for the management and anti-spam filtering of incoming corporate email traffic. IronPort incorporate the technology of partners Dell, Brightmail and Boldfish products.

In addition IronPort offers two services to the email community, the Bonded Sender program and the SenderBase information service. The Bonded Sender program, currently in public beta trial, requires that commercial email senders agree to a set of standards and post a financial bond to ensure the integrity of their email. Recipients who feel they have received an unsolicited email from a bonder sender may complain and a charge is deducted from the bond.

ePrivacy Group

The ePrivacy group is a privately held company providing consulting and training services related to electronic privacy programs and has developed and released software technology and products to combat the spam problem. ePrivacy's technology offerings include "Postiva" which allows the inclusion of trust stamps in volume email and SpamSquelcher which reduces the receipt rate of incoming email traffic identified as spam. The ePrivacy group also jointly administers the "Trusted Sender" program with TRUSTe.

Habeas, Inc.

Habeas is a private company offering Sender Warranted Email[SM], a service to identify email originating from registered users. Senders obtain a license to include a special header containing a copyrighted haiku poem in email that complies with Habeas guidelines. Receiving gateways are expected to interpret incoming email containing the headers as 'not spam'. Should a non-registered user incorporate the special headers, Habeas has promised legal action against copyright infringement.

CipherTrust Inc.

CipherTrust is a private company that provides security solutions to enterprise email systems. Its main product is "IronMail", a secure email gateway appliance that sits between the corporate network firewall and the mail server. IronMail may be configured to include anti-virus, anti-spam, secure webmail access, and secure delivery between email servers using encrypted connections. Anti-spam capabilities include blacklists, whitelist capabilities, content-based filtering, and rules-based header analysis among others.

SpamArrest

SpamArrest is a private company offering a subscription-based anti-spam service to consumers. The SpamArrest service uses a challenge-response mechanism for preventing the receipt of email from automated senders. When an email arrives from an unknown sender, a reply email is sent back asking the sender to verify themselves by clicking on a link to the Spam Arrest website. The link takes them to a page where they are instructed to type in a word that is shown in a picture. This step prevents automated systems, such as those used to send spam, from authorizing themselves, yet is easy for any human to complete. Senders may also be pre-authorized by the end-user to prevent the challenge-response.

Client Based Solutions

The following is a cross section of examples of PC based products for combating spam. The NAI ESPC does not endorse or deny the accuracy or value of any of these or other anti-spam products.

Vanquish

Vanquish is a small private company offering an anti-spam solution similar in concept to the Bonded Sender program. The Vanquish software is installed at the recipient's workstation. When email is received from unknown senders, Vanquish requests an upfront guarantee of payment (through its centralized authentication servers) should the recipient perceive the email as unwanted spam. If the recipient accepts the email (say it is from a legitimate, permission-based list), the sender pays nothing. If not, recipients click a 'Penalty Button' and the Sender is charged a small amount from their guarantee. In this manner, Senders are charged for unwanted bulk email as they would be for bulk postal mail or will refrain from sending the bulk email.

SpamKiller from McAffee Security

A division of Network Associates, Inc., McAffee Security specializes in desktop security products. It retails Spamkiller, an email filtering product with standard filters updated from an on-line service, customizable filters for the end-user, a capability for whitelisting friends, and an abuse complaint reporting capability.

Spam Buster from Contact Plus

Contact Plus retails several Windows-based personal software products. Spam Buster works with POP3 email accounts to filter the email before it is downloaded to the recipient's email client. Spam Buster accesses the email account, compares the email message, header information, sender, and size to the user's spam settings defining the message as spam and also checks the sender against a blacklist of known spammers. Spam Buster then displays the email with a red checkmark indicating they are spam, a question mark if the mail appears to be spam, and those on a local whitelist with a special icon. Messages marked as spam may then be deleted with a single click.

iHateSpam from Sunbelt Software

This product is an email-filtering product specific to MS Outlook, Outlook Express and the Windows operating environment, executing automatically with the operation of the email client software. The filtering mechanism identifies possible spam email and places it in a separate folder inside the mail client for deletion of review by the user. The product supports whitelists of friends, blacklists, and customer filtering rules (in the Outlook version).

Identity Certification Initiatives

VeriSign Inc.

VeriSign is a publicly traded company offering security, internet payment, internet registration and related services. VeriSign is best known as one of the largest SSL Certificate Authorities and offers Digital ID's for digitally signing and encrypting email.

Verisign has released a white paper entitled "A Plan for no Spam" advocating improvements in sender authentication and changes to the SMTP protocol.

US Postal Service – In Person Proofing identity certification program

The U.S. Postal Service formally announced the In Person Proofing (IPP) at Post Offices program to support the activities of US Certificate Authorities and government organizations. Working in conjunction with accredited Certificate Authorities, a process is being developed where applicants for a digital certificate will be required to present themselves in person with hard identification in order to verify their identity. The physical address of the individual will also be validated through the use of the First Class Mail process. From the Federal Register of June 17, 2003:

> "An organization can establish a relationship with a qualified U.S. Certificate Authority to integrate digital signing with improved identity verification into an online application. Any individual desiring to use digital certificates that include USPS IPP will complete an application online. The inline system will verify the individual's identity via commercial database checking. The system will then produce a standard Postal Service form to be printed out at the 'applicant's' personal computer. The individual requesting the service will present this form to a participating post office where the 'In Person Proofing' process is conducted. After successful completion of the IPP event, the CA will notify the applicant to download their digital certificate."

About the NAI's Email Service Provider Coalition:

The Email Service Provider Coalition (ESPC) was formed in November 2002 by the Network Advertising Initiative (NAI) to fight spam while protecting the delivery of legitimate email. The ESPC is comprised of 37 members including aQuantive, Blue Dolphin, Digital Impact, DoubleClick, Experian, IMN, and Roving Software. The ESPC members have recognized the need for strong spam solutions that ensure the delivery of legitimate email. To this end, the ESPC has created several crucial sub-committees, including legislative and technical committees, which have been very active in the war against spam. Our flagship initiative, Project Lumos, is an industry proposal for a registry-based solution to the spam problem. For more information on the ESPC, please visit www.projectlumos.com.

Founding Members:

Avenue A	Blue Dolphin Group	Digital Impact
DoubleClick	Experian	IMN
Roving Software		

Members:

@Once	Acxiom	Advertising.com
AFG Media	BlueHornet Networks, Inc.	BlueStreak
Britemoon	CheetahMail	ClickAction
Digital Connexxions	eDialog	Eversave
ExactTarget	Got Marketing	Mediaplex
Mindshare Design	NetCreations	Performics
Postfuture	Quris	Responsys
SKYLIST	SmartSource	SourceLink
Topica	Traffix, Inc.	Transend
Virtumundo	WebSideStory	

The Work of the NAI ESPC:

Email is indeed a "killer app" and has been a major component in the productivity and efficiency gains of the digital economy. But those gains will be lost if email becomes unreliable as a communications tool. According to a report by Assurance Systems, in the first half of 2003, subscribers to the major ISPs did not receive an average of 17% of permission-based email. Businesses will not be able to use email if they cannot have a reasonable assurance that their messages will be delivered. Simply stated, a 17% failure rate for delivery of email is not tenable for communications with customers.

The ESP Coalition is currently working on many fronts to address the spam problem and, at the same time, ensure the continued delivery of permission-based email. We have groups that are working on technological solutions, groups working with the ISPs to refine filtering tools, and groups working to ensure that consumers are aware of the problem of false positives. The Coalition is also working to educate public policy makers on the need for balance in any legislative or regulatory solutions to the spam problem. Again, it is critical that we have strong tools in place to fight spam, but those tools cannot be so blunt as to damage the legitimate use of emails in today's marketplace.

Appendix B

ESPC

Email Service Provider Coalition

Email Marketing Pledge

1. **Unsolicited Commercial Email**

   Unsolicited commercial email must not be sent.

2. **Commercial Email**

   a. **Commercial email** must not be sent to an individual's e-mail address unless one of the following situations exists:

      i. There is an existing **business relationship**; or

      ii. Prior **informed consent** of the individual has been obtained.

3. **Content of Commercial Email**

   a. Every commercial email must include an opportunity for the recipient to **unsubscribe** from receiving such email in the future. Such requests to unsubscribe must be processed promptly and the recipient should be informed of the length of time required for processing.

   b. Commercial email must not include "from address" fields, subject lines and message bodies that are misleading, false, or deceptive. Subject lines must not mislead as to the content and purpose of the message.

4. **Gathering of Email Addresses**

   a. Email addresses must not be gathered through surreptitious methods (e.g., scraping or harvesting).

Definitions:

Commercial Email: email messages, sent in volume, the primary purpose of which is the commercial advertisement or promotion of a product or service.

Business Relationship: A relationship between the sender of an email message and the recipient. Such a relationship may be created through the facilitation or completion of a commercial transaction between the sender and a recipient. A business relationship may also be created through prior correspondence initiated by an individual, including requests for information, responses to questionnaires or surveys, responses to sweepstakes or contests, or offline contact.

Informed Consent: A mechanism through which an individual is clearly and fully notified of the collection and use of an email address and has consented prior to such collection and use. Informed Consent may be implemented in the following forms:

- **Opt-in:** At the point of email address collection, a person has affirmatively requested to be included on an email list to receive commercial email. No confirmation email is sent and the person is not required to take further action to be included on the email list.

- **Confirmed Opt-in:** At the point of email address collection, a person has affirmatively requested to be included on an email list to receive commercial email. An email is subsequently sent to the person, notifying the person that their email address has been added to the email list. The person is not required to take further action to be included on the email list.

- **Double Opt-in:** At the point of email address collection, a person has affirmatively requested to be included on an email list to receive commercial email. An email is subsequently sent to the person, notifying the person that some action is necessary before their email address will be added to the email list.

Unsubscribe: A mechanism through which an individual may request that he or she no longer receive commercial email.

Unsolicited Commercial Email: Commercial Email sent without an existing business relationship or prior informed consent.