The Marketers' Guide to Accreditation, Reputation and Authentication Resources

Increasingly, a marketer's email "reputation" will play a significant role in determining whether or not email is delivered. In addition to following industry best practices, marketers can take specific steps that can improve their "reputation" and maximize deliverability and ROI.

The following are critical elements for building positive email reputation:

- **ISP whitelists and automated feedback loops:** ISP-level tools to help identify "good" senders and facilitate email delivery – reputation at the local level.
- **Authentication:** technology protocols that establish the true identities of senders and allow for the development of a sender's email reputation.
- **Accreditation Services:** 3rd-party programs that certify sender policies and practices and contribute to a sender's email reputation.
- **Reputation Services:** monitors that gather all available data intelligence on senders and aggregate a global reputation score

These charts were co-created by the Email Service Providers Coalition (ESPC) and the Interactive Advertising Bureau (IAB) as a helpful guide for marketers navigating the offerings available today.

The charts that follow are representative and accurate at the time this document was created. It is possible that, through the course of business, these details will change. We will do our best to keep in this information updated and available on the IAB website (http://www.iab.net). Please note, these charts should not be considered an exhaustive list of all the available vendors and ISPs. Please contact the ESPC (Jim Campbell, campbell@espcoalition.org) with any updates.

ISP Usage of Email Authentication, Feedback Loops and Whitelists

The chart below shows which ISPs have adopted email authentication protocols, are implementing automated feedback loops, and/or whitelists. Each of these provides a tool through which email senders can work with ISPs to improve email deliverability.

	Authentication							Whitelisting		
ISP	Status	Type	Version	Filter	Notification		Feedback loop	Whitelist	Delivery impact	Filters used
					Pass	Fail				
Adelphia	NA	None	None	No	NA	NA	No	No	None	Brightmail
AOL (aol.com)	Publishing	IP	SPF/Sender-ID	No	None	None	Yes	Standard	Whitelisted mail not guaranteed to go to inbox	DNS check, volume, feedback, reputation
AOL (aol.com)	Publishing	IP	SPF/Sender-ID	No	None	None	Yes	Enhanced	Whitelisted mail not guaranteed to go to inbox, but delivered with links and images intact	DNS check, volume, feedback, reputation
ATT.net	NA	None	None	No	NA	NA	No	No	None	Brightmail, limits, proprietary blacklist
CompuServe (compuserve.com)	Publishing	IP	SPF/Sender-ID	No	None	None	Yes	Enhanced	Whitelisted mail not guaranteed to go to inbox, but delivered with links and images intact	DNS check, volume, feedback, reputation
Netscape (netscape.com)	Publishing	IP	SPF/Sender-ID	No	None	None	Yes	Enhanced	Whitelisted mail not guaranteed to go to inbox, but delivered with links and images intact	DNS check, volume, feedback, reputation
Bellsouth (bellsouth.net)	Verifying	IP	SPF	No	None	None	No	No	None	Proprietary filter, proprietary blacklist
Charter (charter.net)	Publishing	IP	SPF	No	None	None	No	No	None	NA
Comcast (comcast.net)	Publishing	IP	SPF	No	None	None	No	No	None	Brightmail, proprietary blacklist
EarthLink (earthlink.net, mindspring.com, peoplepc.com)	Publishing	Crypto	DK	No	None	None	No	No	None	Brightmail, external blacklists
Excite	NA	None	None	No	NA	NA	No	No	None	Proprietary blacklist

Status:
Verifying: ISP is checking for existence of authentication on incoming email
Publishing: ISP is publishing SPF/Sender ID record for outgoing mail
Signing: ISP is attaching a DK signiture to outgoing email
Testing: ISP is evaluating either inbound or outbound authentication protocols

Filter:
Indicates if ISP weighting authentication (positively or negatively) in delivering messages. This is an ongoing process in which ISPs are increasingly adopting authentication standards and determining how to treat incoming email based on the usage of those standards.

Notification:
Pass: ISP provides notification to recipient that message has passed an authentication check.
Fail: ISP provides notification to recipient that message has failed an authentication check.

Type:
IP based: validating the source (IP address) of message
Crypto: validating the sender (signature) of message

Source:
ISP data: ISP Postmaster sites and Deliverability.com (February 2006)
Authentication data: ISP Interviews (ESPC, April 2006)

ISP Usage of Email Authentication, Feedback Loops and Whitelists (con't)

The chart below shows which ISPs have adopted email authentication protocols, are implementing automated feedback loops, and/or whitelists. Each of these provides a tool through which email senders can work with ISPs to improve email deliverability.

	Authentication							Whitelisting		
ISP	**Status**	**Type**	**Version**	**Filter**	**Notification**		**Feedback loop**	**Whitelist**	**Delivery impact**	**Filters used**
					Pass	**Fail**				
Google (gmail.com)	Verifying/Publishing/ Signing	IP/Crypto	SPF/DK	Yes	Yes	Yes	No	No official safelist	None	Image blocking
Juno/NetZero (netzero.net, juno.com)	Publishing	IP	SPF/Sender-ID	No	None	None	Yes	Yes	Whitelisted mail not guaranteed to go to inbox	
Microsoft (msn.com, hotmail.com)	Checking/Publishing	IP	SPF/Sender-ID	Yes	Yes	Yes	SmartNetwork Data Services (SNDS)	Sender Score Certified and Habeas	Sender Score Certified mail generally achieves consistent delivery to inbox, as does successful implementation of authentication	Proprietary filter (SmartScreen), Brightmail
RoadRunner (rr.com)	Publishing	IP	SPF	No	None	None	No	Sender Score Certified and Habeas	None	Multiple 3rd party blacklists
Verizon (verizon.net, gte.net, bellatlantic.net)	Publishing	IP	SPF	No	None	None	No	Yes	Safelist process does not guarantee placment in inbox or bypassing of Brightmail filter	Proprietary blacklists, Brightmail
Yahoo! (yahoo.com)	Verifying/Signing	Crypto	DK	Yes	Yes	Yes	No	Yes	Whitelisted senders can still end up in bulk folder	
*SBCGlobal (sbcglobal.net)**	Verifying/Signing	Crypto	DK	Yes	Yes	Yes	No	Yes	Whitelisted senders can still end up in bulk folder	
Britsh Telecom (btinternet.com)	Verifying/Signing	Crypto	DK	Yes	Yes	Yes	No	No	None	NA
Rogers Cable (rogers.com)	Verifying/Signing	Crypto	DK	Yes	Yes	Yes	No	Yes	Whitelisted senders can still end up in bulk folder	

Status:
Verifying: ISP is checking for existence of authentication on incoming email
Publishing: ISP is publishing SPF/Sender ID record for outgoing mail
Signing: ISP is attaching a DK signiture to outgoing email
Testing: ISP is evaluating either inbound or outbound authentication protocols

Filter:
Indicates if ISP weighting authentication (positively or negatively) in delivering messages. This is an ongoing process in which ISPs are increasingly adopting authentication standards and determining how to treat incoming email based on the usage of those standards.

Notification:
Pass: ISP provides notification to recipient that message has passed an authentication check.
Fail: ISP provides notification to recipient that message has failed an authentication check.

Type:
IP based: validating the source (IP address) of message
Crypto: validating the sender (signature) of message

Source:
ISP data: ISP Postmaster sites and Deliverability.com (February 2006)
Authentication data: ISP Interviews (ESPC, April 2006)

ISP Usage of Email Authentication, Feedback Loops and Whitelists (con't)

The chart below shows which ISPs have adopted email authentication protocols, are implementing automated feedback loops, and/or whitelists. Each of these provides a tool through which email senders can work with ISPs to improve email deliverability.

	Authentication							Whitelisting		
ISP	**Status**	**Type**	**Version**	**Filter**	**Notification**		**Feedback loop**	**Whitelist**	**Delivery impact**	**Filters used**
					Pass	**Fail**				
Rocket Mail (rocketmail.com)	Verifying/Signing	Crypto	DK	Yes	Yes	Yes	No	Yes	Whitelisted senders can still end up in bulk folder	
International domains (Yahoo UK, CA, Hong Kong, France, India, Twain, Mexico, China, Italy)	Verifying/Signing	Crypto	DK	Yes	Yes	Yes	No	Yes	Whitelisted senders can still end up in bulk folder	
USA.net	NA	None	None	No	NA	NA	No	No	None	Brightmail
Rediff	NA	None	None	No	NA	NA	No	No	None	Spamhaus blacklist
OptOnline	NA	None	None	No	NA	NA	No	No	None	Spamhaus blacklist, Spamcrub proprietary filter, Brightmail
Outblaze	NA	None	None	No	NA	NA	No	No	None	

Status:
Verifying: ISP is checking for existence of authentication on incoming email
Publishing: ISP is publishing SPF/Sender ID record for outgoing mail
Signing: ISP is attaching a DK signiture to outgoing email
Testing: ISP is evaluating either inbound or outbound authentication protocols

Filter:
Indicates if ISP weighting authentication (positively or negatively) in delivering messages. This is an ongoing process in which ISPs are increasingly adopting authentication standards and determining how to treat incoming email based on the usage of those standards.

Notification:
Pass: ISP provides notification to recipient that message has passed an authentication check.
Fail: ISP provides notification to recipient that message has failed an authentication check.

Type:
IP based: validating the source (IP address) of message
Crypto: validating the sender (signature) of message

Source:
ISP data: ISP Postmaster sites and Deliverability.com (February 2006)
Authentication data: ISP Interviews (ESPC, April 2006)

The chart below indicates vendors that provide accreditation services. Typically, vendors put senders through a review process and award accreditation to qualifying applicants. Partner ISPs/receivers deliver accredited mail to end user inboxes.

Company	Basis of Accred.	Accreditation Indices	Data Sources	Ongoing Compliance	IP vs. Domain	Transparency	How filter?*	Delivery impact - users	Delivery impact - non-users	Technical requirements	Blacklists Employed	Coverage	Fees
												(as of date of report)	
Goodmail Systems	Evaluation process	Complaint data, assessment of mailing and data collection practices, identity verification, corporate history	Application data, ISP complaint data, identity and credit verification agencies	Receives and tracks ISP ARF data, monitors unsubscribe requests via proprietary tool	Neither - monitors reputation of sender entity	To sender, receiver, and end user (via Certified Email icon and logo)	By token	Mail with tokens delivered to inbox by participating ISPs. Mail bypasses all filters except user preferences. Links and images are enabled by default. Tokens have no impact on delivery at non-partner ISPs.	Mail without tokens subject to normal filtering	Requires MTA upgrade or installation of imprinter appliance	None	AOL, Yahoo!	Fee for accreditation, plus per message fee for senders
ReturnPath (Sender Score Certified ~ formerly Bonded Sender)	Evaluation of policies and practices, and measured quantitative performance data	Authentication usage, complaint rates, unsubscribe integrity, unknown user rates, spam trap hits, email policy reivew, network integrity and security review	Application, background check, policy review, review of measured quantitative performance data	Daily monitoring of compliance with Quantitative Requirements (use of data from Sender Score, ISP data feeds, Sender Base, SpamCop and Lashback). Policy review where warranted	IP (moving to domain)	To receivers via DNS. To senders via web tool and/or compliance reports	Participating senders are listed on the Sender Score Certified Whitelist	Participating ISPs deliver whitelisted mail with preferential treatment. Participation has no impact on delivery with non-partner ISPs.	Non-certified mail subject to normal filtering	Certified mail sent over dedicated IP. Use of email authentication protocol(s)	Selection of Tier 1 blacklists based on correlation with compromised hosts	Relationships with Hotmail/MSN, RoadRunner, and SpamAssassin. Cover approx. 250 million email boxes.	Free to receivers. Senders pay an Application fee and annual license fee (special arrangements for non-profits).
TRUSTe Email Privacy Seal	Evaluation process	Disclosure review	Application, SenderScore	Watchfire / WebXM scanning	Domain	Consumer facing seal on every online data collection point, EPS seal links directly to seal verification page	NA	None. Participating senders are subject to ISP filtering	None. Participating senders are subject to ISP filtering	None	SpamCop, Spamhaus, Senderbase, Google Abuse	14,000 Domains	Application fee based on volume, license fee based on annual revenue
Habeas (Sender Solutions)	Evaluation process	Authentication usage, complaint rates, email policy review, network integrity and security, unsubscribe integrity, blocklist check, news group check	Application, background check, policy review	Monitor direct complaints, complaints routed through SpamCop, and complaints via feedback loops; blacklist reviews; unsubsribe monitoring	IP	To sender and receiver	Participating senders are listed on a Habeas DNS-based Safelist	Participating receivers deliver mail from Safelisted senders to inbox.Participation has no impact on non-partner receivers	Non-Safelisted mail subject to filtering	None. All SMTP compliant MTAs can support service, including OpenWave, Port25, StrongMail, Sendmail	Spamhaus, SpamCop, approx. 50 other blocklists	Relationships with MSN/Hotmail, Netzero/Juno, RoadRunner, Outblaze, USA.Net, France Telecom. Cover approx. 500 million email boxes worldwide	Vendor does not make fee structure publicly available

** How partner ISPs/receivers filter mail based on a particular accreditation service*

Source:
Goodmail, ReturnPath, TRUSTe, Habeas (April 2006)

The chart below indicates vendors that provide reputation services. Reputation services continuously monitor sender activity and determine a reputation score based on a fixed set of criteria. Partner ISPs/receivers use the reputation score to filter mail for delivery.

Company	Basis of Reputation	Reputation Indices	Data Sources	IP vs. Domain	Transparency	How filter?*	Blacklists employed	Delivery Impact	Technical requirements	Coverage	Fees
										(as of date of report)	
Lashback	Directly observable behavior	Unsubscribe reputation, including failure to honor unsub requests, suppression list abuse, lack of a sufficient or operable unsub mechanism	ISP data, feedback data	IP	Scores available to senders and receivers via UnsubMonitor tool	Based on reputation score	Proprietary DNS-based blacklist - lists senders who have misused suppression lists	Participating ISP/receivers filter based on reputation. Higher scores do not guarantee delivery to inbox. May be used in conjunction with other filters.	None	NA	Set up fee plus monthly maintenance fee based on the number of IPs or unsubscribe links monitored
ReturnPath (Sender Score Reputation Monitor)	Directly observable behavior	60 datapoints from receivers to develop composite reputation, incl. complaints, filtering, volume, network integrity, ID stability, unsub reputation, sending stabiliity, 3rd party reputation, authentication	ISP logs, filtering services, public data, 3rd party reputation sources	IP (moving to include domain)	Receivers via DNS. Senders via a web tool.	Based on reputation score	Select Tier 1 blacklists based on correlation with compromised hosts	Participating ISP/receivers filter based on reputation. Higher scores receive preference, but does not guarantee delivery to inbox. May be used in conjunction with other filters.	None	40mm+ mailboxes	Free to receivers. Senders can receive top level scores for free via DNS. Additional information is availbe for a yearly subscription fee.

** How partner ISPs/receivers filter mail based on a particular reputation service*

Source:
Lashback, ReturnPath (April 2006)

Glossary

Accreditation: Third-party whitelist programs that certify that mail from certain senders has gone through a rigorous review process and has been "certified" as safe for delivery.

Authentication: The practice by ISPs and other mail gateway administrators to establish the true identity of the sender. Examples of proposed authentication standards include: DomainKeys, DKIM, SPF, and Sender ID.

Blacklist (public): A list of IP addresses believed to send spam. Created and held by third parties; sometimes used by ISPs as a filtering mechanism to block email delivery.

Blacklist (proprietary/private): A list of IP addresses believed to send spam. Created and held by ISPs, mail filtering software providers, and some reputation and accreditation service providers and used as a filtering mechanism to block email delivery.

Sender Policy Framework (SPF): Authentication standard that specifies what IP addresses can send mail for a given domain. Requires change to DNS records to implement.

SenderID: Authentication standard based on SPF that expands the verification process to include the purported responsible address (PRA) included in the header. Requires change to DNS records to implement.

DomainKeys (DK): Authentication standard that "signs" each outgoing message with an encrypted key. Requires changes in how messages are constructed to implement.

DKIM: Enhanced encrypted authentication standard that combines Domain Keys and Identified Internet Mail standards. Requires changes in how messages are constructed to implement.

Filters: Methods by which ISPs and other message receivers attempt to separate "good" messages from spam and phishing attacks. The variety of filters employed is widely varied, and includes blacklists, whitelists, 3rd party software, reputation scores, accreditation, subject line and content review and more.

Feedback loop: An automated system by which ISPs provide approved senders with direct feedback about mail sent into a particular system. The feedback typically is restricted to spam complaints and opt-out requests.

MTA: Mail Transfer Agent. A computer program or software agent that transfers electronic mail messages from one computer to another.

Transparency: In the context of this document, the ability to access reputation and accreditation data by senders, receivers, or consumers.

Whitelist: A list of trusted IP addresses and domains that generally allows all mail from these addresses to be delivered, bypassing some or all spam filters. Senders typically go through a review process of some sort before being placed on a whitelist. Whitelisted senders can be delisted if their mailing practices fall below the required standard or generate excessive complaints.

Reputation: Reputation services continuously monitor sender activity and determine a reputation score based on a fixed set of criteria. The reputation score changes in real-time with sender activity. Partner ISPs/receivers use the reputation score to filter mail for delivery.

Source:
ESPC (April 2006), Wikipedia (April 2006), "Sign Me Up" by Matt Blumberg, Michael Mayor (2005)