ASP CERTIFICATION REQUIREMENTS

validity

Contents

Introducing Certification 3

Application Service Provider Certification Requirements Overview 5

Part 1: Business Model 5

Part 2: Measurability 7

Part 3: Infrastructure 9

Part 4: Email Message Content 11

Part 5: Privacy Policy 12

Part 6: Legality 12

Part 7: Security 13

Part 8: Feedback Loops (FBLs) 14

Part 9: Communication 14

Part 10: Performance and Compliance 15

Need help? 16

Introducing Certification

The Validity ASP Sender Certification program provides access to exclusive data feeds and ongoing support from a team of Certification experts for the duration of your contract, in addition to the opportunity to become a Certified sender. Once you fulfill the necessary requirements to demonstrate your emails can be trusted and achieve Certified sender status, we will place your IP address(es) on our allowlist, and our mailbox provider partners will be notified of this change. Your placement on the allowlist will also start Validity's 24x7 monitoring of your IP address(es) to protect against security threats that could damage your sender reputation.

An Application Service Provider (ASP) is an entity contracted to send transactional emails on behalf of third-party companies. ASPs typically support communications for businesses in a specific industry or vertical (finance, insurance, healthcare, etc.) and send email content that is similar in scope for all their clients.

An ASP contracted to send transactional emails on behalf of third-party companies is the responsible party for Certification purposes. The ASP is accountable for any action (or inaction) or activity, including of or by the ASP's clients, which results in suspension or termination of Certification benefits. This includes, but is not limited to IP and domain blocklisting's, email content, etc.

During any time your IP addresses are not Certified, you will still have access to the data feeds and our Certification experts will remain available to provide coaching on the changes needed to achieve Certification.

Customer Responsibilities

Sender Certification Questionnaire

Customers are required to complete the Sender Certification questionnaire ("Questionnaire") and are responsible for submitting the completed questionnaire to their Certification Analyst. The completed questionnaire enables your access to the data feeds and kicks off your email program audit for Certification. It is in your best interest to complete the Sender Certification questionnaire as soon as possible. Typically, customers are able to complete this within the first day.

The Validity Certification team will work quickly to review your responses, perform the audit of your email program, and compile a summary of any findings preventing you from becoming Certified. Any issues identified in this review are the responsibility of the customer to resolve in order to proceed with Certification.

Certification Maintenance

Customers are required to continuously fulfill the conditions set by the program to retain Certification status. The specified conditions will ensure you are aware of and adhering to industry standards and demonstrating your ability to be recognized as a trusted sender.

Become Certified

ASP Sender Certification is designed to provide deliverability protection for reputable senders that follow industry-standard best practices and meet subscribers' as well as top mailbox providers' expectations. Throughout your process to become Certified, we will work together to ensure your program fulfills our program requirements.

By applying for ASP Certification, you represent that your responses to the ASP Certification program are complete and accurate. Throughout the process, we may ask for additional information to confirm your email program meets ASP Certification requirements. You must provide this information before you can become Certified, and promptly notify Validity of any changes.

Here are the key steps to becoming Certified:

1. When you subscribe to ASP Sender Certification services, we will initiate a comprehensive audit of your email program, as requested, to ensure your program meets all the requirements detailed below.

2. You will be asked to provide our Certification Team with details about your email program. Once received, you will gain access to your deliverability data direct from our mailbox providers and filtering agency partners. This data will provide you with details on how your IP addresses have performed by allowing you to monitor complaint rates, spam trap hits, sending volume and more.

3. If your email program meets the requirements outlined in the Business Model, Measurability, and Infrastructure sections below, your account may be eligible for preliminary activation of the Certified status before the audit is complete.

4. If your program qualifies for preliminary activation, you will receive Certification benefits including access to Certification Program features and services for up to 60 days while we conduct our audit and you work on the required updates to become Certified.

5. During the audit, we will notify you if any parts of your email program do not meet our requirements and provide you with additional information on the changes and how to complete them. We recommend you complete any updates as soon as possible to ensure you are using the full services available within your subscription.

6. If your audit updates are not complete after the 60-day preliminary activation period or your IPs do not meet the requirements for Certification at any point during your subscription, your IP(s) will be suspended from the Certification allowlist. If suspended, you will still have access to your Certification data outlined above and we will continue to work with you and give guidance on corrections to be made to complete the audit and be re-activated to the Certification allowlist once all corrections are made.

7. Once all appropriate changes are made, the Certification team will finalize your audit and your certified IP addresses will be added to the allowlist.

Application Service Provider Certification Requirements Overview

To become and stay Certified, you will need to meet the requirements of the ASP Certification program. These requirements are based on best practice guidance established in partnership with our mailbox provider partners.

Breaking Down the Requirements

- **Business Model:** Be transparent about who you are and what you do
- **Measurability:** Send email in volumes and at frequencies that appeal to your recipients
- **Infrastructure:** Properly send, authenticate, and manage email
- **Email Message Content:** Present yourself distinctly and accurately to your recipients
- **Privacy Policy:** Document all the details of your email program
- **Legality:** Adhere to any applicable spam and data privacy laws that impact you and your recipients
- **Security:** Show how you take care of your systems and recipients' data
- **Feedback Loops (FBLs):** Use complaint feedback to keep a clean, healthy list of subscribers
- **Communication:** Communicate timely, clearly, and openly with Validity
- **Performance and Compliance:** Demonstrate your email program stays within performance thresholds established by mailbox providers and subscribers

Part 1: Business Model

Your business model gives us important information about your overall email program and helps us determine if you're a good fit for ASP Certification. Here are the requirements your business model must meet to become and stay ASP Certified:

1. Business Registration

- Your business is verifiable by a public third-party source through a legitimate online website, such as a country registry, or an application such as Dun & Bradstreet.
- Your business registration includes your business's current physical address.
- Your business has been operational and legally registered for at least one year.
- Your business does not use a registered agent to obscure any of your business's information.

2. Website

- Your website(s) use Hypertext Transfer Protocol Secure (HTTPS).
- The root domain of all sending domains associated with your Certified IP(s) must lead to a valid, operable website clearly identifying you or your ASP client.
    - Note: A redirect to a valid, operable website clearly identifying you or your ASP client is sufficient.

3. IP Addresses and Content

- Certified IP addresses must be dedicated to you, the ASP. Shared IP addresses are not eligible.
- Certified IPs can only send transactional email as defined below.
    - Action Validation: Automated, real-time messages sent to users after a specific action is performed. This type of email validates an action a user has taken; therefore, focuses on the information pertinent to that user's action. Examples include account creation confirmations, double-opt in verification or confirmation emails, password reset requests, and order confirmations.
    - Obligatory Notifications: Involuntary notifications required to be sent by law or regulation and advise or alert users about essential information. Examples include legal advisories, security alert notifications, recall announcements, and privacy policy notices.
    - Transaction Completion: Messages directly related to a recent transaction's life cycle. These emails provide a customer with necessary information about the status of a recent transaction. Examples include shipping confirmations, invoices, payment notifications, and surveys.
        - Note: Surveys are only Certifiable if they are intended to complete a recent transaction's life cycle, typically defined as within 30 days of the event for which the survey applies. Surveys cannot be company-generic and must be directly related to a specific, recent transaction that has taken place.
- Certified IPs must send templated, clearly branded emails. We define templated email as pre-designed email campaigns that contain text, images, logos, and other information related to the Certified Sender's identity, products and services. Templated emails cannot contain free-form content such as input from web forms or open text boxes.
    - This means you cannot use Certified IPs to send corporate email, which often includes internal communications between co-workers or customer support emails.

IMPORTANT: We do not Certify businesses in any of the following categories:

Market Research & Survey Companies	Companies performing research on behalf of others in order to test the interest, opinion of or to obtain feedback from target audiences or consumers.
Aggregators	Companies collecting various pieces of information from third parties and combine the content into single mailings.
Email Service Providers (ESPs), Agencies, Third-party Mailers, etc.	Companies sending promotional mailing on behalf of brands they do not fully own. Including, but not limited to, ESPs, Marketing Agencies, White-Labels, Affiliate Mailers, etc. However, companies sending transactional mail on behalf of their clients is allowed.
Lead Generation	Companies collecting email addresses for the purpose of growing sales pipeline, prospecting, etc. for brands not fully owned by the Certified entity.
List Rental Providers	Companies compiling permission-based email lists and sell access to them for brands to send email marketing campaigns to.
Penny Bid Auction	Online retailers offering one cent bidding to their customers.
Illegal Activities	Business operations or practices that may violate the law in a given jurisdiction.
Human Trafficking	Businesses operating for the purpose of illegally transporting people from one area to another.

Part 2: Measurability

Measurability helps us understand your overall sending patterns, including how often you're sending to your recipients. Here are the measurability requirements you must meet to become and stay ASP Certified:

1. Measurable and consistent volume

- Each IP address sends at least 100 email messages to each Microsoft and Yahoo! over the most recent 30-day period, as seen in Validity's data sources.
- Each IP address maintains a measurable and consistent volume to remain Certified. Consistency is determined based on your particular program and sending behavior.
- IP addresses without measurable and consistent volume are not eligible for review.
- Once Certified, IP addresses without measurable and consistent volume will be suspended after 30 days and deleted from the program after 90 days.

2. Targeting mailbox providers

- Your business cannot use a single IP address to send email to one specific mailbox provider.

Occasional and temporary single-receiver mailings may be tolerated under certain circumstances. Validity must approve any exceptions in writing in advance.

3. IP Segmentation

- IP Segmentation is the process of separating and sending email traffic from different IP addresses based on various factors related to your email program such as domains, region and mail type. The objective of IP segmentation is to organize your mail in such a way as to maximize performance to help ensure your email reaches the inbox. While not required, we highly recommend implementing an IP segmentation strategy for your email program. Learn more about IP segmentation here.

4. Sending volume and IP limits

- Certified customers are limited in the number of IPs that can be associated with their account. The table below reflects the maximum number of IPs allowed in Certification based on your contracted annual sending volume.

Sending Volume (Annually)	Maximum # of IPs
1,200,000	2
3,000,000	2
7,500,000	3
12,000,000	4
36,000,000	5
60,000,000	6
90,000,000	7
120,000,000	8
180,000,000	9
240,000,000	10
420,000,000	13
600,000,000	16
1,200,000,000	18
> 1,200,000,000	22

Part 3: Infrastructure

Infrastructure refers to the hardware and process used to deploy email. It's crucial you send email from well-maintained infrastructure systems using best practices. Keep in mind you may need to work with your Email Service Provider (ESP) or internal IT team to comply with the requirements listed below to become and stay ASP Certified:

1. Dedicated IP Addresses

- IP addresses are dedicated to you, the ASP, and are used for at least 60 days to send transactional emails on behalf of your clients.

2. Open Relays

- Your infrastructure does not have any open relay servers.

3. FCrDNS

- Your IP address reverse DNS (rDNS) entry matches the forward DNS entries, otherwise known as Forward-Confirmed reverse DNS (FCrDNS).

4. SPF

- All Return-Path and Sending domains used in conjunction with Certified IP addresses must have Sender Policy Framework (SPF) records. Learn how to set up SPF here.
- Your SPF records pass mailbox provider authentication checks within reasonable operational tolerance as determined by Validity.
- SPF records do not use a +all or ?all directive.
- SPF records to not use a pointer (PTR) mechanism.

5. DKIM

- All of your email sent over Certified IPs are DomainKeys Identified Mail (DKIM) signed. Learn how to set up DKIM here.
- Your DKIM authentication pass mailbox provider authentication checks within reasonable operational tolerance as determined by Validity.
- DKIM Keys have a minimum of 1024 bits. For additional security, we recommend 2048 bit key length.
- The DKIM length tag (l=) is the number of characters from the message body that were used to compute the body hash (bh=). If this value isn't present, then it's assumed the whole message body was used. Including the length (l=) tag in your DKIM signature is not recommended for Certified senders as bad actors can exploit this vulnerability and modify your messages to include malicious content. If you are using the (l=) tag in your DKIM signature, we suggest removing it from your emails. You can replace the (l=) tag with the (x=) tag, which allows you to set an expiration time for the DKIM signature.

6. DMARC

- You publish Domain-based Message, Authentication, Reporting & Conformance (DMARC) for each domain that sends mail from your Certified IPs. Learn how to set up a DMARC record here.
- DMARC must be set to at least p=none and in alignment with SPF and/or DKIM. However, all three policy flags (p=none, p=quarantine and p=reject) are acceptable within Certification.
- The authenticating domain must be the same domain found in the message From: header.
- The authenticating domain must have a "rua" value for processing aggregated reports from mailbox providers. It is recommended to monitor these reports either through Everest or through other DMARC reporting tools.

7. ARC

- If operating a forwarding service of any kind, we highly recommend implementing Authenticated Received Chain (ARC). ARC is an email protocol that helps preserve email authentication results and verifies the identity of email intermediaries that forward a message on to its final destination. Learn more about ARC here.

8. Role Accounts

- You operate functional abuse@ and postmaster@ role accounts for all Return-Path and Sending domains to handle complaints and other issues.
- We also recommend you support and maintain other standard role accounts such as support@ or help@ accounts.

9. Domain Ownership

- Sending domains used in conjunction with Certified IPs must be owned by and registered to you or your ASP client.
- Your business must have full access and control over all Return-Path domains, associated with the email sent from your IP addresses.
- To verify domain ownership and control over domains associated with your Certified IP(s), you or your ASP client may be required to update the DNS with a TXT record containing a unique character code provided by Validity.
    - This TXT record is required to remain within your or your ASP client's DNS record for the duration of your membership in the Certification program.

10. List Hygiene

- Your ASP clients must own and supply their mailing lists to you, the ASP. The mailing lists cannot belong to or originate from you.
- You are responsible for maintaining the quality of your clients' mailing lists and ensuring that email addresses are properly validated.
- Your business uses email address list maintenance systems to reliably receive and process delivery errors, bounce messages, and other replies from receiving networks.
- You process hard bounces from emails sent over your IP addresses by removing the undeliverable email address from all future mailings.

11. Transport Layer Security (TLS)

- TLS is an industry-standard protocol primarily used for encrypting communication between web applications and servers for security and privacy reasons. We recommend using a TLS connection for transmitting email from Certified IPs.

Part 4: Email Message Content

We review your email message content to ensure that your email follows best practices as expected by mailbox providers. This includes being transparent with your recipients about who you are. Here are the email message content requirements you must meet to become and stay ASP Certified:

1. Branding

- All emails sent over Certified IPs must include clear branding identifying either you or your ASP client. Including the branding of both parties is recommended as a best practice.
- Text-only mail must include the following information for either you or your ASP client: o Website URL
    - Company name
    - Brand's standard signature
    - Valid physical mailing address

2. Subject Line

- All subject lines are accurate.
- All subject lines clearly relate to the email body content without being deceptive or misleading.
- No subject lines include "RE:" or "FWD:". Using these abbreviations is typically seen as a deceptive tactic prompting recipients to open the email as if it were sent from an individual rather than a commercial sender.

3. Email Body Content

- All email body content is truthful and accurate.
- All emails sent over Certified IPs must include the physical address of either you or your ASP client.
- URL shorteners are prohibited in your message content. This includes, but is not limited to, the use of Bitly or TinyURL.
- Links within the message body should be visible and easy to understand. Recipients should know what to expect when they click a link.
- Do not use a Report Spam link within your email body's content. This is typically used by senders who attempt to avoid mailbox provider complaints.
- Don't use HTML, CSS, or other tactics to hide content in your messages for spam filter interference.
- Attachments, regardless of file type, within any Certified mail are not permitted.

4. Message Headers

- The From address and Friendly From name clearly identifies you or your ASP client.
- Email message headers are not falsified, obscured, deceptive, or misleading in any way. Message header identifies such as the Return-Path header, the From header, the Friendly From name and address must be accurate and operable.
- Message headers should be RFC Compliant including:
    - Every message includes a valid Message-ID
    - No repeat use of single instance message headers in a message
    - All messages should be compliant with RFC5322 message formatting.
- Avoid excessively large message headers

Part 5: Privacy Policy

It's important to note your privacy policies must adhere to any laws applicable to you in you in your operating jurisdictions. Your business should be fully transparent with potential subscribers about what data you collect, your email program, and how they can reach you. These are the privacy policy requirements you must meet to become and stay ASP Certified.

1. Easily Accessible

- Your company must have a valid privacy policy that is easily accessible on your website's homepage.

2. Physical Address

- Your privacy policy includes a current physical address for your company. P.O. boxes are acceptable, although recipients prefer street addresses. If your physical address is not present in your privacy policy, Validity requires it be found either on the homepage or the contact us page of your website.

3. Data Disclosure

- Your privacy policy must tell recipients about all personal information your business collects and how it might be shared.

4. Brand Ownership

- If you are a brand owned by a parent company, you must include the name of the parent company and your relationship with that entity in your privacy policy.

Part 6: Legality

Each country and territory has legislation related to email and data practices. It is the Customer's responsibility to understand, fully comply with, and follow these laws and regulations wherever you operate. Validity is not responsible for determining if a Customer's program is legal. Customer's presence on the

allowlist is not a determination that Customer's program is operating legally. A Customer's failure to comply with the laws, however, will preclude them from participation in the ASP Certification program. Examples include, but are not limited to:

United States of America:

- Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM)
- State Specific Legislation

Canada:

- Canada's Anti-Spam Legislation (CASL)

Europe:

- General Data Protection Regulation (GDPR)
- ePrivacy Directive
- UK General Data Production Regulation (UKGDPR)

Australia:

- Spam Act of 2003

Brazil:

- Brazillian General Data Protection Law (LGPD)Part 9: Security

Part 7: Security

It's important your business takes adequate, industry-standard steps to keep your database and systems secure so you can protect your infrastructure and your subscribers. Here are the security requirements you must meet to become and stay ASP Certified:

1. Infrastructure

- Your email infrastructure is maintained and operated in a responsible, reliable, and security-conscious manner.

2. Subscriber protection

- Your business uses adequate, industry-standard policies and procedures to secure and protect your subscribers' email addresses and other personal data.

3. Secure systems

- Your business uses industry-standard efforts to prevent open proxies, open relays, computer viruses, worms, spyware, adware, trojans, recursive DNS, or any other item identified as malware on your infrastructure.

4. Compromises

- You will notify Validity in writing within 2 business days if you discover your IP or domain has been compromised.
- If your IP or domain is compromised, you agree that the IP or domain will not be re-enabled in the Certification program until Validity completes a review and determines that the cause of the compromise has been properly mitigated.

Part 8: Feedback Loops (FBLs)

As a best practice, we recommend you sign up for all available feedback loops (FBLs) in order to effectively manage and reduce complaints. A full list of FBLs can be found here. If for some reason you aren't able to sign up for the entire list of FBLs, here are the feedback loops you must sign up for to become and stay ASP Certified:

- Microsoft Junk Email Reporting Program
- Comcast IP and Domain Feedback Loop
- Yahoo! Feedback Loop

Part 9: Communication

Whether you are just beginning the Certification application process or you're already Certified, it's important there is clear and open communication between your business and Validity. Here are the communication requirements you must follow in order to become and stay ASP Certified:

1. Issue Resolution

- To resolve any Certification program-related issues, you and any team involved in sending email will cooperate with the Certification administrators.
- You respond to any program notice within 3 days, and initiate any required actions within 10 days of the notice.

2. Contact Information

- You maintain up-to-date contact information with Validity.

Part 10: Performance and Compliance

When you remain within the performance thresholds listed below, you receive reputation benefits at participating mailbox providers, improving your deliverability to reach more of your subscribers. Exceeding any thresholds will result in suspension in part or in whole.

Note: We actively work with our partners to determine thresholds and suspensions.

You must meet the following performance requirements in order to become and stay ASP Certified:

Individual IP Microsoft SRD Compliance Thresholds (30-day cumulative)

SRD Volume	0-4	5-10	11 or More
SRD Rate	Not Enforced	5 Junk Votes	45%

Microsoft Group SRD Compliance Thresholds (30-day cumulative)

SRD Volume	0-9	10-30	31-50	51 or more
SRD Rate	Not Enforced	75%	65%	55%

Note: IPs that have 1 or more junk votes will be suspended if the Group SRD thresholds have been exceeded. Group SRD enforcement occurs when your total Certified IP count is greater than or equal to 2.

Tip: Having problems with your Microsoft SRD rates? Check out these resources.

Complaint Compliance Thresholds (30-day average of all sending volumes)

Microsoft: Complaint Rate	0.2%
Yahoo!/AOL: Inbox Complaint Rate	0.2%
Comcast: Complaint Rate	0.3%
Cloudmark: Complaint Rate	1.0%

Tip: Having problems with your complaint rates? Check out this resource.

Note: Certification only enforces mailbox provider complaint rate thresholds if you receive a minimum number of complaints at specific mailbox providers:

- **Microsoft:** 200 complaints
- **Yahoo!:** 200 complaints
- **Comcast:** 100 complaints
- **Cloudmark:** 100 complaints

Spam Trap Compliance Thresholds (30-day cumulative)

Critical Spam Traps	3 Trap Hits
Significant Spam Traps	5 Trap Hits
RP Trap Network	100 Trap Hits
Cloudmark Traps	100 Trap Hits

Tip: Having problems with spam hits? Check out this resource.

Blocklist Compliance Thresholds (current listing)

Critical Blocklist	1 Blocklisting
Significant Blocklist	2 Blocklistings

NOTE: Repetitive or excessive blocklistings may result in the suspension or termination of your Certification benefits. Learn more about the blocklists that we monitor here.

Need help?

For additional insight into Certification and its requirements, or to learn how to troubleshoot deliverability and reputation issues, visit our Help Center.

For over 20 years, tens of thousands of organizations throughout the world have relied on Validity solutions to target, contact, engage, and keep customers – using trustworthy data as a key advantage. The Validity flagship products – DemandTools, BriteVerify, Everest, GridBuddy Connect, and MailCharts – are all highly rated solutions for CRM data management, email address verification, inbox deliverability and avoiding the spam folder, and grid CRM applications. These solutions deliver smarter campaigns, more qualified leads, more productive sales, and ultimately faster growth.

For more information, visit Validity.com and connect with us on LinkedIn and X (formerly known as Twitter).

validity.com

sales@validity.com