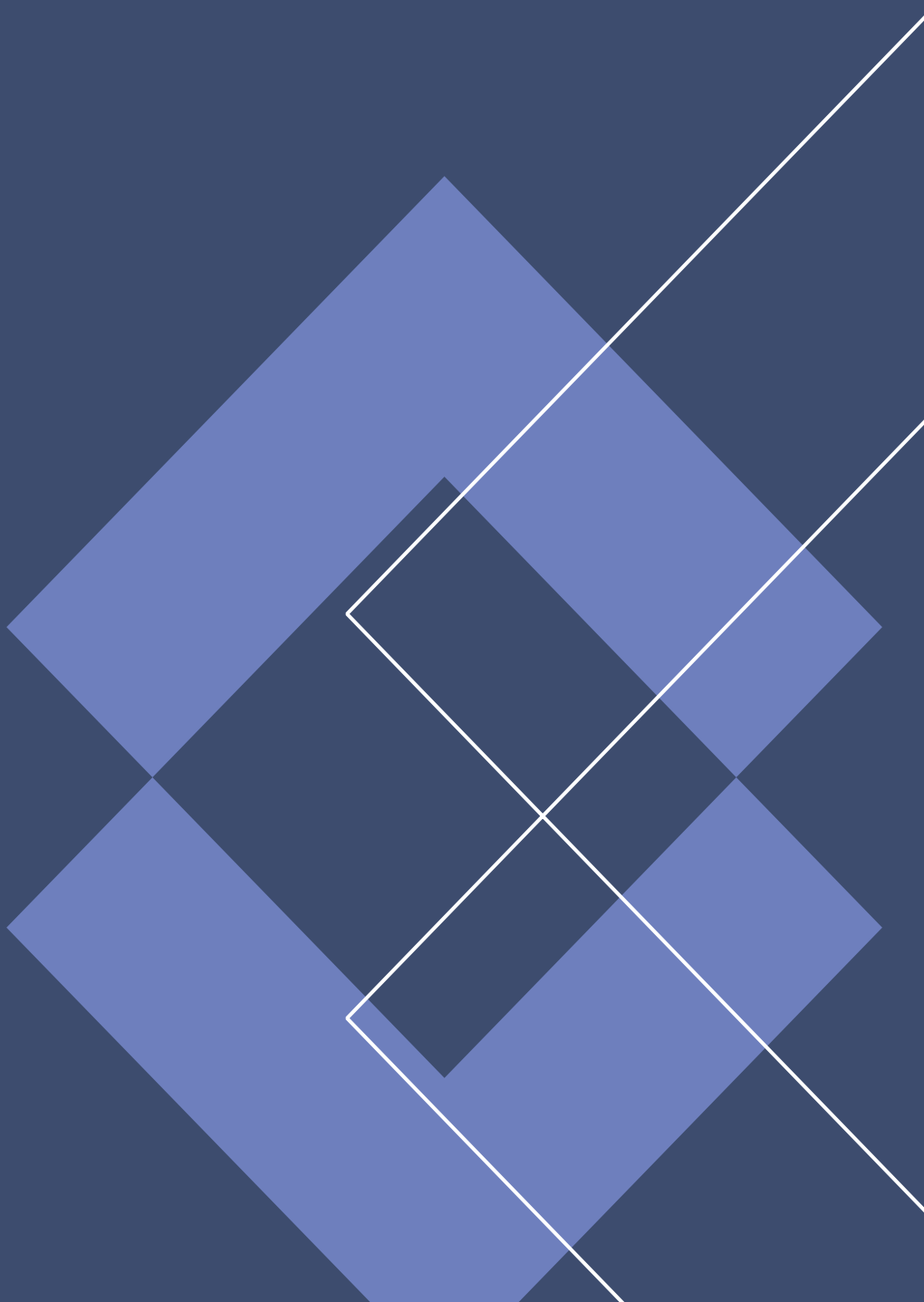
CSA
Certified Senders Alliance

Criteria

for IP platform certification by the Certified Senders Alliance (CSA)



Criteria

for IP platform certification by the Certified Senders Alliance (CSA)

Table of Contents

1. Mandatory criteria 4

1.1 Trust and transparency 4
1.1.1 Company contact information 4
1.1.2 Privacy information on the website 4
1.1.3 Compliance with relevant RFC standards 4

1.2 Abuse prevention 4
1.2.1 Abuse / complaint contact address 4
1.2.2 Measures for platform providers sending emails for third parties 4
1.2.3 Protection of customer accounts 4
1.2.4 Deactivation of redirect links in case of abuse 5
1.2.5 Implementation of the X-CSA-Complaints header 5
1.2.6 Technical security of outgoing mail servers 5
1.2.7 TLS-secured email transmission 5

1.3 Authentication 5
1.3.1 SPF for MAIL FROM 5
1.3.2 DKIM signature 5
1.3.3 DKIM alignment 6

1.4 List hygiene 6
1.4.1 List-Unsubscribe and List-Help header 6
1.4.2 Opt-out option in marketing emails 6
1.4.3 Unsubscribe link for email sending platform providers 7
1.4.4 Bounce handling 7
1.4.5 Handling of non-existent mailboxes 7

1.5 Reputation and performance indicators 7
1.5.1 Spam complaint rate 7
1.5.2 DKIM missing rate 7

Criteria

for IP platform certification by the Certified Senders Alliance (CSA)

1.5.3 Hard bounce rate 7
1.5.4 Additional reputation indicators 7

2. Recommended criteria/general recommendations 8
2.1 Registration for feedback loops and CFBL header 8
2.2 Multipart emails (HTML + text version) 8
2.3 Implementation of DMARC 8
2.4 Implementation of DANE or MTA-STS 8
2.5 DKIM key length and signature algorithm 8
2.6 Double opt-in procedure 9
2.7 Information about mailing frequency 9
2.8 Reply-to address 9
2.9 Separation of newsletter and transactional email IPs 9
2.10 Avoidance of URL shorteners 9
2.11 Extended DKIM alignment 9

1. Mandatory criteria

1.1 Trust and transparency

1.1.1 Company contact information

The company[1] must provide its postal address and a digital contact option in the form of an email address or contact form that is easy to find on its website.

1.1.2 Privacy information on the website

The company must ensure that easily accessible privacy information is available on its associated website. This information must indicate when and to what extent personal data (both from customers and end users) is collected and processed. It must also include details of the measures taken to protect personal data from misuse.

1.1.3 Compliance with relevant RFC standards

Every email sent (structure and composition) and the email delivery (envelope communication in SMTP dialogue) must comply with the relevant Request for Comments (RFC) of the IETF.

The current RFCs are authoritative. At the time of writing, these include RFC 6532, 2142, 2369, 5321, 5322, 7208, 6376 and 8058.

1.2 Abuse prevention

1.2.1 Abuse / complaint contact address

The company is obliged to set up a general abuse or complaint address under its organisational or company-related domain and to register this in the CSA's Certification Monitor. This address must be a role account and should preferably have the structure abuse@org-domain.tld. The company must be able to respond to messages from the eco Complaints Office within 24 hours on business days.

1.2.2 Measures for platform providers sending emails for third parties

If the company offers email technology for sending commercial bulk emails as a service to third parties, it must implement appropriate measures to ensure compliance with CSA criteria, including in relation to individual customers. This includes, for example, blocking access, limiting sending speed, the maximum permitted volume or restricting the maximum number of sending domains.

1.2.3 Protection of customer accounts

If the company offers email technology for sending commercial bulk emails as a service to third parties, it must implement appropriate security measures to protect its customers' accounts from access by unauthorised third parties (e.g. two-factor authentication).

[1] The term "company" refers to the participant in the certification process or the certified company of IP-Platform-Certification.

1.2.4 Deactivation of redirect links in case of abuse

If redirect links are used in sent emails, the company must be able to immediately deactivate these links or have them deactivated in the event of misuse (e.g. when sending phishing emails) in order to prevent or limit damage caused by these links.

In the event of notification by the eco Complaints Office that redirect links are being misused for phishing or similar purposes, deactivation must be carried out on working days within 24 hours at the latest.

1.2.5 Implementation of the X-CSA-Complaints header

Once certification has been completed, an "X-CSA-Complaints" header must be inserted and DKIM-signed. An implementation period of four weeks is granted for this, beginning with the notification of successful certification. The header line is: "X-CSA-Complaints: csa-complaints@eco.de" and may only be implemented on the certified outgoing email server. Fulfilment of this criterion must be confirmed to the CSA by means of a test mailing.

1.2.6 Technical security of outgoing mail servers

The company's outgoing email servers must be technically secured by appropriate measures (e.g. with a firewall, no open relay, no public proxy, no backscatter, continuously monitored servers, etc.).

1.2.7 TLS-secured email transmission

Emails must be delivered to the recipient via a Transport Layer Security (TLS)-secured connection in accordance with the current state of the art.

1.3 Authentication

1.3.1 SPF for MAIL FROM

An SPF entry (RFC 7208) must be stored for the MAIL FROM address specified in SMTP communication between the email servers. This enables the outgoing email server to be authenticated to the receiving email server. The SPF entry must end with "-all" or "~all".

1.3.2 DKIM signature

Every outgoing email must contain at least one valid DKIM (Domain Keys Identified Mail) signature in accordance with RFC 6376.

For companies that provide a technical platform for sending commercial mass emails as a service for third parties, the following applies: The domain used in the "d=" tag must be assignable to the company's customer, i.e. it must correspond to the customer's sending domain. Additional DKIM signatures for the company's own domains (DKIM double signature) are permitted.

For companies that use their own technical platform for sending commercial mass emails, the following applies: The domain used in the "d=" tag must be assignable to the company itself, i.e. it must correspond to its sending domain.

In all cases, the DKIM signature must include at least the header fields "From", "X-CSA-Complaints", "Date", and "To". The use of the length parameter "l=" is not permitted.

1.3.3 DKIM alignment

Every outgoing email must contain a DKIM alignment and provide at least one "relaxed alignment". For a "relaxed alignment", the organisational domain part of the DKIM signature ("d=" tag in the signature) must match the RFC5322.From (header From) domain in order to achieve the required alignment.

Example:

```
DKIM-signature: v=1; ...; d=brand.com; ...
From: „Friendly From“ local-part@subdomain.brand.com

or

DKIM-signature: v=1; ...; d=subdomain.brand.com; ...
From: „Friendly From“ local-part@brand.com
```

If the company offers a technical platform for sending commercial mass emails as a service to third parties, an exception to DKIM alignment is permitted if no brand-related, company-related, or organisation-related domain (or subdomain) of the customer exists.

1.4 List hygiene

1.4.1 List-Unsubscribe and List-Help header

The company must offer the functionality to insert a "List-Unsubscribe" header and a "List-Help" header in every email. The subsequent selection of the appropriate header depends on the content of the email to be sent and is not the responsibility of the IP platform–certified company.

The "List-Unsubscribe" header must be able to be inserted using the URL method (in accordance with RFC 2369) with a "POST HTTPS" link. This must be able to be combined with the "List-Unsubscribe-Post" header, which supports the "One-Click-Unsubscribe" functionality (RFC 8058).

The "List-Help" header must contain at least one "mailto:" address or an HTTPS link; HTTP links are not permitted. Both the use of the "mailto:" address and the HTTPS link must give the recipient the opportunity to obtain information about why the email was sent to them and why unsubscribing at list level is not possible.

1.4.2 Opt-out option in marketing emails

In every email of an advertising nature, it must be possible for the recipient to unsubscribe from further emails without a separate login (unsubscribe/opt-out). The company must therefore ensure that every email sent contains a corresponding functional unsubscribe option. This requirement does not apply to emails of a non-advertising nature (especially transactional emails).

A link should preferably be used as the unsubscribe option; alternatively, the provision of an email address is permissible.

1.4.3 Unsubscribe link for email sending platform providers

If the company offers a technical platform for sending commercial mass emails as a service to third parties, it must provide its customers with a technical functionality that allows them to insert an easily recognisable and functional unsubscribe link in every email (in the email body). It is permissible for the unsubscribe link to lead to a selection page where the scope of the unsubscription can be specified (e.g. unsubscription from all company newsletters or only from individual newsletters, unsubscription from newsletters on specific topics, etc.).

1.4.4 Bounce handling

The company must be able to receive bounce messages during SMTP transmission in accordance with RFC 5321 and process them for the purpose of list hygiene. To enable this bounce handling, it must set up an MX record for the envelope-from (mail-from) domain. Alternatively (as a fallback), an A record is also permitted.

1.4.5 Handling of non-existent mailboxes

The company must prevent further delivery to email addresses where it is determined after delivery that the mailbox does not exist.

1.5 Reputation and performance indicators

1.5.1 Spam complaint rate

The spam complaint rate per mail server (IP address) or per company may not exceed 0.3 per cent within a period of seven days (one week). The spam complaint rate is calculated as the ratio of the number of spam complaints by recipients to the number of emails in the inbox.

1.5.2 DKIM missing rate

The average DKIM missing rate for a company may not exceed 3.0 percent within a period of seven days (one week). The DKIM missing rate is calculated as the ratio of the number of emails with DKIM missing to the total number of emails sent. This threshold only includes data from data partners who provide data for DKIM validation.

1.5.3 Hard bounce rate

The average hard bounce rate per mail server (IP address) or per company may not exceed 1.0 per cent within a period of seven days (one week).

1.5.4 Additional reputation indicators

Furthermore, the company should not have any significant reputation problems (IP- or DKIM-based) with participating mailbox or security providers (e.g. based on spam trap hits, content scanners or high spam rates).

2. Recommended criteria/general recommendations

2.1 Registration for feedback loops and CFBL header

The company should register for the publicly accessible feedback loops of mailbox and security providers. It is also recommended to implement the CFBL header (RFC 9477).

2.2 Multipart emails (HTML + text version)

HTML-formatted emails should generally be extended with a text part (MIME). This should contain unsubscribe information and notes about the newsletter, as recipients may not always be able to receive HTML-formatted emails correctly.

2.3 Implementation of DMARC

It is recommended to use Domain-based Message Authentication, Reporting and Conformance (DMARC) in accordance with RFC 7489 so that mailbox providers as recipients can check the received emails according to the specified parameters. When using DMARC, reporting email addresses must be specified in such a way that reports sent by mailbox providers can be processed by the company or its customer(s). It is recommended to use a "reject" policy.

2.4 Implementation of DANE or MTA-STS

The company should implement DANE in accordance with RFC 7671 to ensure secure email delivery. This requires DNSSEC in accordance with RFC 9364 to be available for the sender and recipient domains.
If DNSSEC is not available in the long term, MTA-STS in accordance with RFC 8461 should be used instead to at least secure transport encryption.

2.5 DKIM key length and signature algorithm

It is recommended to use DKIM keys with a length of at least 2,048 bits. SHA-256 should be used as the signature algorithm.

2.6 Double opt-in procedure

It is strongly recommended that user data be collected using the double opt-in (DOI) procedure in order to meet the strict requirements of the GDPR regarding the obligation to provide evidence. A confirmation email sent in this context must not contain any advertising or other content.

2.7 Information about mailing frequency

It is recommended that, when collecting the email address (e.g. when subscribing to a newsletter), information about the expected frequency of mailings be provided, if a frequency exists or is planned.

2.8 Reply-to address

It is recommended that a functional reply-to address be explicitly stated in every email. Alternatively, a functional sender address should be used so that the recipient can contact the sender using the "reply" function.

2.9 Separation of newsletter and transactional email IPs

It is recommended that newsletters and transactional emails be sent via different IPs.

2.10 Avoidance of URL shorteners

For reasons of transparency, the use of URL shorteners is not recommended.

2.11 Extended DKIM alignment

It is strongly recommended to extend DKIM alignment (see above, criterion 1.3.3) to the Mail-From header (RFC5321).

Example:

```
DKIM-signature: v=1; ...; d=example.com; ...
MAIL FROM: xyz@foo.example.com
From: "Example" <sender@child.example.com>
```

In addition, it is recommended to ensure consistency for the list header (RFC4021), reply-to header (RFC5322) and, if available, sender header (RFC5322) with one or the same DKIM signature, also at the organisational level.