Email Authentication

The protective shield for your domain and door opener to your inbox

Publisher:

DDV German Dialogue Marketing Association, DDV
eco – Association of the Internet Industry

CSA
Certified Senders Alliance

Table of contents

1. Executive summary

Did you know?

- Since February 2024, **Gmail and Yahoo** have required all senders of 5,000 or more emails per day to use SPF, DKIM and DMARC, as well as an easy-to-use unsubscribe option.
- **Microsoft** followed suit in 2025 with similar requirements for Outlook consumer domains.
- The **aim of these measures** is to reduce the scope for fraudsters and improve the quality of emails in inboxes.

Facts

The threat situation is dramatic. Hornetsecurity examined 45 billion emails from 2023. The results showed that 36.4 per cent were unwanted and 3.6 per cent were clearly malicious – that's over 589 million dangerous messages in just one year. Phishing accounted for 43.3 per cent of all attacks, the highest rate ever measured (source: Hornetsecurity).

Kaspersky recorded over 893 million blocked phishing attempts worldwide in 2024, which is an increase of 26 per cent over the previous year (Kaspersky 2025). Almost all industries were affected, particularly web services, internet portals and banks, retail, delivery services and social networks.

The economic consequences are serious. According to Bitkom, cyberattacks caused 267 billion euros' worth of damage in Germany in 2024 alone. This includes direct loss of revenue, disruption to IT systems, legal costs and long-term reputational damage (source: Bitkom 2024).

Consequence

Email authentication is no longer just a technical option. Today, it is the ticket to the inbox. Companies that do not implement SPF, DKIM and DMARC correctly risk being blocked, suffering reputational damage and incurring financial losses.

Recommendation

This white paper explains how companies can use SPF, DKIM and DMARC to lay the foundation for secure communication, what organisational and technical hurdles need to be overcome, and why monitoring is becoming a strategic early warning system. It makes it clear that email authentication is mandatory and that partners such as the Certified Senders Alliance (CSA) are key to establishing long-term trust and ensuring stable deliverability through transparency.

2. Introduction

> **Executive Insight: E**mail authentication is mandatory. Without it, there is a risk of spam, blockages and abuse.

Email is the backbone of modern business communication. It is fast, inexpensive and universally applicable. At the same time, it is one of the biggest gateways for cyberattacks. Without authentication, emails run the risk of ending up in the spam folder or being rejected by the receiving server.

Even more serious is the threat of your brand being misused. Attackers send deceptively genuine phishing emails on behalf of companies to persuade recipients to disclose sensitive data. The consequences are damage to your image, legal risks, and a loss of trust that is difficult to regain.

In this white paper, produced in cooperation between the Certified Senders Alliance and the German Dialogue Marketing Association (DDV), you will learn:

- why authentication is essential in email delivery,
- what risks exist if it is not implemented,
- how SPF, DKIM and DMARC work and interact,
- what typical stumbling blocks to be aware of,
- and how monitoring and partners such as the CSA provide companies with sustainable support.

The aim is to provide specialists and managers in IT, marketing and management with a clear basis for decision-making. The white paper combines technical explanations with practical recommendations and shows that email authentication is not just an IT issue, but a business-critical success factor.

3. Email caught between communication and threat

> **Executive Insight:** Email is indispensable – and at the same time the most widely used attack vector.

Email is more important to companies than any other means of communication. It conveys information, brand messages and transaction data. This is precisely what makes it a preferred target for attackers.

The major mailbox providers have responded. Since February 2024, Gmail and Yahoo have required consistent authentication and clear unsubscribe mechanisms for high mail volumes

(Google, Yahoo 2024). In April 2025, Microsoft announced similar requirements for Outlook consumer domains (source: Proofpoint 2025).

The threat situation is measurable: Hornetsecurity analysed 45 billion emails from 2023. 36.4 per cent were unwanted and 3.6 per cent were malicious. Phishing was the most common form of attack at 43.3 per cent (source: see above).

The danger is also increasing globally. Kaspersky recorded over 893 million blocked phishing attempts in 2024, which is an increase of 26 per cent over the previous year. All industries were affected, especially web services, internet portals and banks, but also retail and social networks (source: Kaspersky 2025).

The economic damage is enormous. In Germany alone, losses due to cyberattacks amounted to 267 billion euros in 2024. This figure includes direct financial losses as well as damage to reputation and legal costs (source: see above).

Interpretation: Companies that do not use authentication risk not only spam filter problems, but also their reputation, their turnover and the security of their customers.

4. What does email authentication mean?

> **Executive Insight:** Authentication is proof of identity in email correspondence. It confirms the sender and protects recipients from manipulation.

Email authentication enables the receiving server to verify that a message has actually been sent by the specified sender and has not been altered during transmission. Three standards are central to this process: **SPF**, **DKIM** and **DMARC**.

- **SPF** specifies which servers are authorised to send emails on behalf of a domain.
- **DKIM** digitally signs each email and to ensure that the content remains unchanged.
- **DMARC** combines both methods, sets rules for how recipients should handle faulty messages, and provides reports on anomalies.

While authentication alone does not prevent all attacks, it is the foundation for secure communication. Companies that use SPF, DKIM and DMARC correctly are classified as trustworthy by mailbox providers, thereby improving their chances of delivery to the inbox.

Interpretation: Authentication is to email what a passport is to humans – proof of identity and integrity. Without this proof, access is denied.

5. The consequences of inadequate or missing authentication

> **Executive Insight:** Lack of authentication leads to abuse, delivery problems and financial damage.

The risks are concrete and manifold:

Brand abuse and phishing

If a domain is not protected, attackers can send deceptively genuine-looking emails on behalf of the company. Customers can then be tricked into revealing sensitive data. This directly associates the brand with fraud.

Loss of trust

Phishing incidents in the name of a company leave their mark – on social networks, in the press, with customers and partners. Regaining trust is costly and time-consuming.

Delivery problems

Missing or incorrect authentication results in emails being blocked or sent to the spam folder. Messages that are not read are ineffective.

Loss of business

Important transactional emails, such as invoices or password resets, may not reach the customer. This can lead to abandoned purchases, lost revenue, and an increased number of service requests.

Legal consequences

Phishing and data breaches can result in fines, claims for damages and legal costs.

Interpretation: Without authentication, companies lose not only emails, but also their reputation, revenue and legal certainty.

6. The three cornerstones of email authentication

> **Executive Insight:** SPF, DKIM and DMARC together form the foundation of a secure email infrastructure.

SPF – the guest list for mail servers

An SPF record in the DNS specifies which servers are allowed to send emails on behalf of a domain. The receiving server checks whether the message comes from an authorised source.
Risk: Outdated or overly broad entries create vulnerabilities.

DKIM – the digital seal

DKIM provides each email with a digital signature. Like a seal on an envelope, it shows whether the message is unchanged. The public key is stored in the DNS, while the private key remains with the sender.
Risk: Insufficient key length or lack of rotation weakens security.

DMARC – the bouncer with a rule book

DMARC combines SPF and DKIM and specifies how recipients should handle emails that fail the check. Three modes are available:

- **none**: Observe without intervention,
- **quarantine**: suspicious messages end up in spam,
- **reject**: unauthenticated emails are consistently rejected.

In addition, DMARC provides reports showing which servers send emails on behalf of a domain, whether they are authorised or not.

Interpretation: Only the interaction of the three standards creates effective protection. SPF checks the source, DKIM checks the integrity, DMARC decides on the course of action. Together, they form a protective shield against abuse.

7. Typical stumbling blocks and how to avoid them

> **Executive Insight:** The biggest hurdles are not technical, but organisational: lack of knowledge, unclear responsibilities, legacy systems.

Many companies fail to implement SPF, DKIM and DMARC not because of the technology, but because of structures and processes. Five stumbling blocks occur particularly frequently:

Lack of awareness

The relevance of email authentication is underestimated. Risks such as phishing or delivery problems are only taken seriously when it is too late.

Recommendation: Raise internal awareness. Train employees in IT, marketing and compliance.

Technical complexity

SPF, DKIM and DMARC require DNS knowledge and a precise understanding of the sending infrastructure. Even small configuration errors can block legitimate emails.

Recommendation: Bring in external expertise if necessary.

Outdated systems

In IT landscapes that have grown over time, it is often unclear which systems are still sending emails. After mergers or tool changes, old delivery paths remain unsecured.

Recommendation: Start by taking stock. Prioritise central sending sources.

Incorrect understanding of security

Firewalls or encryption are mistakenly seen as a substitute for authentication. However, they do not protect against domain abuse.

Recommendation: Establish authentication as an independent part of your security strategy.

Lack of coordination

There is often a lack of coordination between IT, marketing, customer service and compliance. This results in gaps in authentication or blocked legitimate emails.

Recommendation: Establish fixed processes for communication between all parties involved.

Interpretation: Authentication is not an IT project, but a cross-organisational process. Sustainable implementation can only be achieved if responsibilities are clearly defined.

8. Basics of implementation: How to do it right

> **Executive insight:** Three steps ensure effective authentication: analysis, setup and monitoring.

Step 1: System analysis

The first step is to take stock. Which systems send emails on behalf of your domain? These include traditional mail servers, marketing platforms, CRM systems and external service providers. Even domains that appear to be inactive must be taken into account – otherwise they become easy targets.

Questions you should ask:

- Which systems send emails on behalf of our domain?
- Do external providers use our sender addresses?
- Are there any domains that are not currently in active use?

Step 2: SPF – the guest list for mail servers

SPF determines which servers are authorised to send emails for your domain. An SPF entry in the DNS works like a guest list: only those who are listed are accepted.

An example:

v=spf1 ip4:192.0.2.0/24 include:_spf.google.com -all

Common errors:

- Outdated entries that do not reflect new servers
- too broad definitions of entire network ranges,
- exceeding the limit of ten DNS queries.

Step 3: DKIM – the digital seal

DKIM provides each email with a digital signature. Like the seal on an envelope, it shows whether the message has been altered in transit.

Important recommendations:

- minimum key length of 2048 bits,
- Regular key rotation,
- signature across all relevant headers,
- Avoid using the "l=" parameter, as it allows manipulation.

Step 4: DMARC – the bouncer at the entrance

DMARC combines SPF and DKIM and specifies how email servers should handle messages that fail the checks.

Three policies are available:

- none: observation without intervention,
- quarantine: messages end up in the spam folder,
- reject: unauthenticated messages are blocked.

An example:
v=DMARC1; p=quarantine; rua=mailto:reports@domain.de

Practical recommendation:

- Start with "none" to collect initial data.
- gradually switch to "quarantine" and "reject" once all sending sources are known,
- activate reporting functions to detect misuse.

Setting up SPF, DKIM and DMARC is not a one-off project, but a process. Regular checking, surveillance and readjustment will ensure sustainable security.

9. Real data and monitoring – the key to effective and secure email delivery

> **Executive Insight:** Monitoring is the early warning system for security and deliverability. Without data, abuse remains invisible.

Why monitoring is crucial

Setting up SPF, DKIM and DMARC does not guarantee email security. What happens afterwards is crucial. Monitoring reveals which systems are sending emails on behalf of a domain, whether intentionally or not.

DMARC reports as a control tool

Mailbox providers deliver so-called aggregate reports. These show:

- which IP addresses sent emails on behalf of your domain,
- whether SPF and DKIM passed the check,
- where errors or anomalies occur.

These reports are machine-readable and difficult for humans to understand. That is why it is worth using specialised tools that analyse and process the data.

Performance and reputation

Monitoring is not only a security tool, but also a tool for better delivery. Important metrics are:

- spam complaint rates,
- delivery rates,
- hits in spam traps.

A poor reputation leads to mailbox providers blocking messages. A good reputation increases the chance of reliably landing in the inbox.

Recommended actions

- Activate DMARC reports for all domains.
- Use monitoring tools that present reports in an understandable way.
- Respond immediately to any anomalies in the key figures.

Interpretation: Monitoring is not a luxury. It is the nervous system of email security. By continuously monitoring data, you can detect attacks, ensure deliverability, and protect your brand's reputation in the long term.

10. Why a partner is worthwhile: The Certified Senders Alliance (CSA)

> **Executive Insight:** For 20 years, the CSA has been the neutral authority for secure email delivery – with practical data, expertise and a strong network.

The Certified Senders Alliance (CSA) is a joint project of **eco – Association of the Internet Industry** and the **German Dialogue Marketing Association, DDV**. It was created from the insight that email communication can only remain reliable if senders and mailbox providers can rely on uniform standards.

The CSA Certification Monitor

At the heart of the CSA is the Certification Monitor. It provides real data directly from mailbox and security providers – no estimates, no third-party analyses. This allows companies to see how their emails are actually rated.

Key metrics include:

- Spam Complaint Rates,
- Spam Trap Hits,
- Authentication errors such as invalid DKIM signatures or missing alignment.

This data serves as an early warning system for senders. Anomalies can be identified and corrected before systematic blockages occur.

Added value for certified senders

Certified companies benefit from:

- Individual feedback from CSA experts in technology and law
- Notifications of complaints or anomalies in sending behaviour,
- Support with technical and legal questions,
- Access to a community of senders, providers and specialists,
- The CSA certificate as a recognised mark of quality in the market.

Advantages for DDV members

Members of the DDV also benefit from special conditions for CSA certification.

Interpretation: CSA is more than just a certifier. It is an interface, data supplier and partner. Companies that use CSA increase their delivery rates, reduce risks and gain the trust of customers and post office box providers alike.

11. Email authentication is mandatory – for you too

> **Executive Insight:** Authentication is no longer optional, but mandatory. Without it, you will lose access to your inbox.

Whether you are a startup, SMEs or a large corporation, every company that sends emails is affected. The major mailbox providers have made authentication mandatory. Anyone who does not implement SPF, DKIM and DMARC correctly runs the risk of their messages no longer being delivered.

The consequences are clear:

- **Not doing it is not an option.** Without authentication, emails will be blocked or sorted out.
- **Half measures are not enough.** SPF alone does not provide adequate protection. Only the combination of DKIM and DMARC provides security.
- **The timeframe has expired.** Gmail and Yahoo established the facts in 2024. Microsoft followed suit in 2025.

Interpretation: Authentication is now as commonplace as SSL encryption on websites. It is the ticket to the inbox and a prerequisite for trust. Companies that fail to act now risk being excluded from the most important communication channel in the digital economy.

12. Glossary of important terms

SPF (Sender Policy Framework)
A DNS text entry that specifies which mail servers are permitted to send emails on behalf of a domain. The receiving server checks whether the incoming email comes from an authorised mail server. It protects against spoofing, but is not sufficient on its own.

DKIM (DomainKeys Identified Mail)
A process whereby every outgoing email is provided with a digital signature. The private key signs the email, while the public key is stored in the DNS entry. The receiving server then checks that the signature matches and that the email has not been altered en route.

DMARC (Domain-based Message Authentication, Reporting and Conformance)
An extension of SPF and DKIM which specifies rules for how receiving mail servers should handle emails that are not authenticated or are incorrectly authenticated. DMARC also provides reports on the authentication results. There are three policies: *none*, *quarantine*, *reject*.

Alignment
Consistency between the visible sender address ("From") and the domain that has been validated via SPF and/or DKIM. Without alignment, DMARC fails, even if SPF or DKIM are correct on their own.

RUA / RUF (Reporting Addresses for DMARC)

- **RUA (Aggregate Reports):** Daily, machine-readable reports showing which servers are sending emails on behalf of a domain and whether they have been correctly authenticated.
- **RUF (Forensic Reports):** Detailed individual reports on failed authentications. These are used less frequently as they contain potentially sensitive data.

Aggregate Reports
Standardised DMARC reports in XML format that contain collected information (e.g. for 24 hours) about sending sources, SPF/DKIM results and failed attempts. Difficult for humans to read, so evaluation tools are recommended.

Forensic Reports
Detailed reports that may contain individual message fragments in the event of a failed DMARC check. Often not activated for data protection reasons.

Sender reputation
The "reputation" of a sender domain or IP address with mailbox providers. It is based on spam

complaints, delivery rates, bounce rates, authentication status, and other factors. A poor reputation can lead to blocking.

Spam trap
A "trap" set by mailbox providers or anti-spam services: email addresses that have never been actively used or no longer exist. If they are written to, this is considered a sign of poor list quality.

Phishing
An attempt to trick recipients into revealing confidential information (passwords, payment details, etc.) through fake emails. This is often done by spoofing the sender's name (domain spoofing).

Spoofing
Falsification of the sender address in an email so that it appears to come from a trustworthy domain. Hardly recognisable without SPF, DKIM and DMARC.

Bounce
Feedback from the receiving server that an email could not be delivered. A distinction is made between *hard bounce* (permanent, e.g. invalid address) and *soft bounce* (temporary, e.g. full mailbox).

Blocklisting
Inclusion of a domain or IP address in a block list maintained by spam blocking services or mailbox providers. This usually results in emails being blocked or ending up in spam.

Allowlisting
The opposite of blocklisting: a domain or IP is classified as trustworthy, so emails are more likely to be delivered.

TLS (Transport Layer Security)
Encryption for the transmission of emails between mail servers. Ensures that messages cannot be read in plain text during transport. Complements but does not replace SPF/DKIM/DMARC.

MTA-STS (Mail Transfer Agent Strict Transport Security)
A relatively new standard that enforces that emails are only transmitted via TLS-encrypted connections. Increases security in addition to authentication.

BIMI (Brand Indicators for Message Identification)
A standard that enables companies to display their brand logo in the inbox next to authenticated emails. This requires consistent implementation of DMARC with *p=quarantine* or *p=reject*.

About the Certified Senders Alliance

The Certified Senders Alliance (CSA) is a service provided by eco – Association of the Internet Industry and was established in 2004 in cooperation with the German Dialogue Marketing Association, DDV. The CSA acts a neutral interface between mailbox providers and senders of commercial emails. Its aim is to improve the quality of commercial emails (e.g. newsletters, invoices, order confirmations, etc.). To achieve this goal, it establishes legal and technical quality standards. These standards are based on applicable law and the technical requirements of mailbox providers. They are regularly updated in line with current legislation and market requirements.

Authors

Sandra Schubert
Customer Success Manager
Certified Senders Alliance
eco – Association of the Internet Industry

Franz Peter Altemeier
Managing Director
DDV German Dialogue Marketing Association

Julia Janssen-Holldiek
Director
Certified Senders Alliance
eco – Association of the Internet Industry

Legal notice

DDV German Dialogue Marketing Association, DDV

Hahnstraße 70
60528 Frankfurt
Germany

Tel: +49 69 401 276 500
Email: info@ddv.de

Register of Associations, District Court (Amtsgericht) Cologne, VR 15630
VAT identification number: DE 113821908

Board: Martin Nitsche (President), Patrick Tapp (President), Ulf Uebel (Vice President Finance)

Managing Director: Franz Peter Altemeier

eco – Association of the Internet Industry

Certified Senders Alliance
Lichtstrasse 43h
50825 Cologne
Germany

Tel: +49 221 70 00 48-0
Email: info@certified-senders.org
https://certified-senders.org/

Register of Associations: District Court (Amtsgericht) Cologne, VR 14478
VAT identification number: DE 182676944

Board: Oliver Süme (Chair), Klaus Landefeld (Vice Chair), Silke Kanes, Felix Höger, Prof. Dr. Norbert Pohlmann

Managing Directors: Alexander Rabe, Andreas Weiss