Email Authentication in the Financial Sector:

Protection Against Cyber Threats and Ensuring Inbox Delivery

Publisher:
eco – Association of the Internet Industry
Certified Senders Alliance

Author:
Sandra Schubert
Customer Success Manager, Certified Senders Alliance

CSA
Certified Senders Alliance

Email Authentication in the Financial Sector

Protection Against Cyber Threats and Ensuring Mailbox Delivery

In today's fast-paced and digitalised world, communication security is paramount. For many companies, email is a central means of communication in informing customers, staying in contact with them, and managing business processes – including in the financial sector.

In the financial sector in particular – such as in banks and insurance companies – sending commercial emails carries significant risks, both for the company and its customers. The particularly sensitive customer data makes these institutions prime targets for sophisticated email phishing attacks by cybercriminals.

Comprehensive and reliable email authentication is therefore essential to guard against a wide range of cyber threats that can be carried out via email. It not only protects sensitive data, but also ensures reliable delivery of emails – an essential factor in building and maintaining customer trust and safeguarding the reputation of a reputable company in the financial sector.

This guideline highlights the critical role of authentication in securing email communication and outlines the risks that can arise from inadequate implementation. It also presents effective risk management solutions to enhance security and ensure reliable email delivery.

Wishing you happy reading.

1. Email authentication: definition and necessity

Email authentication encompasses protocols and techniques which ensure that emails genuinely originate from the specified sender and have not been tampered with during transmission. In the financial sector, where sensitive customer data is handled on a daily basis, email authentication is particularly important for effectively preventing fraud such as spoofing and phishing.

In email marketing for financial products, email authentication is also a core component and a fundamental requirement for ensuring secure delivery to the recipient's inbox. For mailbox providers such as 1&1, Google, Yahoo or Microsoft, it is the essential factor for spam filter and blocking strategies to protect their users and infrastructure. Furthermore, the authenticated components of an email – IP and domain – are crucial for establishing sender reputation. If a sending domain is abused for spam or phishing, there is a high risk that emails from that domain will be filtered or blocked, which can severely disrupt smooth communication with customers.

Since the beginning of 2024, Google, Yahoo – and soon Microsoft – have been tightening their email authentication requirements to enhance user security. The new, stricter standards for SPF, DKIM and DMARC will result in emails that do not meet the requirements being sent to the spam folder or blocked. You can find more information about these changes and their impact on email delivery here: *https://certified-senders.org/blog/following-csa-criteria-pays-off-yahoo-and-gmail-tightening-their-rules*

2. The financial sector as a preferred target for cyberattacks – the reasons

High value of financial information

Financial data such as account information, transaction histories, and personal identification data are extremely sensitive and highly sought after by cybercriminals. This data provides attackers quick access to money, meaning that financial institutions or insurance companies are particularly attractive targets.

Customer trust in financial institutions

Banks and insurance companies enjoy a high level of trust and a strong reputation, as customers count on their security and reliability in handling sensitive data. Cybercriminals exploit this trust by impersonating these institutions and sending fake emails to deceive customers.

Large customer base and high email volume

The large number of customers in the financial sector increases the likelihood that phishing emails can quickly and easily reach many potential victims. The large daily volume of emails provides cybercriminals with numerous opportunities for phishing attacks. As the methods used become more sophisticated and as emails become more convincing, it becomes challenging for a recipient without technical knowledge to distinguish legitimate emails from fraudulent ones.

3. Risks from a lack of authentication

Negligence in email authentication can have serious consequences:

Loss of customer trust and reputational damage

Phishing attacks can severely undermine customer trust and lead to a significant loss of reputation. Negative media coverage or social media posts about security vulnerabilities or data protection violations create the impression that the company does not adequately protect its customers or lacks the necessary security expertise. This can lead to customer attrition and the loss of potential new customers.

Delivery issues

Customers expect digitalised companies, especially in the financial industry, to reliably deliver important emails such as account updates, contract and policy changes, or account alerts and notifications to their inboxes. However, missing or incorrect authentication can cause these emails to end up in the spam folder or even be rejected entirely by mailbox providers to protect their users. This makes it virtually impossible to communicate with customers on an ongoing basis.

Missed business opportunities

When emails end up in the spam folder or are not delivered, companies lose potential revenue opportunities – as these emails are very unlikely to be seen.

Financial and legal consequences

Potential violations of data protection laws, email delivery issues, or possible customer compensation for losses caused by fraudulent emails, operational disruptions, and increased legal costs from customer lawsuits, can lead to both significant financial and legal consequences.

.

Compromised corporate security

Weaknesses in email authentication can compromise a company's entire IT architecture. Fraudsters can use stolen information to penetrate deeper into corporate systems and cause further damage, threatening the overall integrity and security of the company.

4. Email authentication methods

There are various mechanisms for email authentication that all senders should implement:

SPF (Sender Policy Framework)

SPF is a protocol that allows domain owners to specify which IP addresses are authorised to send emails on behalf of their domain. This enables mailbox providers to check whether an incoming email originates from an authorised source. Emails sent from servers that are not listed in the SPF record fail the SPF check, making them more likely to be sent to the spam folder, as mailbox providers classify them as "not entirely trustworthy".

DKIM (DomainKeys Identified Mail)

A DKIM signature uses a private and public key to verify the integrity of an email. These signatures enable the recipient to check whether the email has been manipulated during transmission. If the message has been modified en route, the recipient will not be able to verify the signature using the public key, and the email will most likely be marked as spam by the mailbox provider or spam filter and delivered to the spam folder.

DMARC (Domain-based Message Authentication, Reporting, and Conformance)

DMARC combines the SPF and DKIM protocols and establishes a policy to determine how the receiving email server should handle emails from a domain that are not authenticated or are incorrectly authenticated. There are three DMARC policies that senders can configure:

"**None**": No specific actions are taken against emails when email authentication fails. It is up to the mailbox provider to assess the risk, and the emails will most likely be delivered as usual. However, a report is generated for the sender to make visible any suspicious activities for the domain and potential threats from any configuration gaps.

"**Quarantine**": Emails that do not pass the authentication check are to be filtered into the spam folder. This reduces the risk of phishing by keeping potentially dangerous emails out of the mailbox, thus significantly restricting the recipient's direct access. There remains a residual risk that recipients will read the emails in the spam folder and may still click on the malicious links contained within.

"**Reject**": When this policy is applied, emails that do not pass the authentication check are already rejected (bounce message) by the receiving server and thus do not penetrate further into the mailbox provider's infrastructure. This reduces the risk of potential phishing attacks, as the emails will not reach the recipient under any circumstances. SPF, DKIM and DMARC are essential for protection against phishing attacks, as they prevent the unauthorised use of domains and thus block or at least significantly impede access to confidential information.

5. Challenges in implementation and approaches to solutions

Lack of awareness

In the banking and insurance sectors, there is often a lack of understanding of the importance of robust email authentication for outbound email communication. Many decision-makers are unaware of the risks of deliverability problems and domain abuse for email spoofing and phishing, as well as their potentially high financial consequences.

Lack of expertise and technical complexity

Many IT employees often lack the necessary expertise and understanding of the complexities required to effectively implement email authentication and avoid typical mistakes.

Outdated systems and complex IT infrastructure

Legacy systems and an increasingly complex IT infrastructure, due to mergers or further developments, make it difficult for companies to implement modern security measures and seamlessly integrate email authentication mechanisms without significant resource expenditure.

Excessive reliance on traditional security measures

Firewalls and encryption are still important, but they only deflect incoming threats to the company itself. However, a firewall does not protect against abuse of the company's domains towards end customers. Email security has two perspectives, and

additional measures are required to ensure more comprehensive protection in both directions.

Lack of cooperation – management of third-party providers

Inefficient internal and external collaboration often leads to interoperability issues and a lack of a holistic approach. Different departments such as IT, marketing and compliance often have different priorities or do not communicate sufficiently with each other.

6. Steps for implementing secure email authentication

Analysis of current email communication and systems

To secure email effectively, it is essential in the first instance to identify where emails are sent, which systems are used, and what IPs and/or domains are utilised. A thorough inventory of the existing security measures for all email servers and sending domains is a fundamental requirement. This forms the foundation for evaluating and planning further actions effectively.

Technical implementation and challenges

For reliable and secure authentication, it is necessary to implement SPF, DKIM and DMARC records in the DNS of all domains. Even domains that are not used for sending emails must be secured against the abusive sending of emails. All records and protocols must be thoroughly tested before applying them to email traffic. In addition, email servers and domains should be continuously monitored.

SPF:
It must be determined which sending servers (IP addresses) are authorised to send emails on behalf of a domain. A corresponding TXT record in the DNS lists these authorised IP addresses.

> **Example SPF record for the domain "company.com":**
>
> ```
> text "v=spf1 ip4:213.165.64.0/23 -all"
> ```
>
> This entry allows emails to be sent from all servers in the 213.165.64.0/23 network range on behalf of the domain "company.com".

Common errors:
SPF records are often not updated regularly, which means that new sending servers are not correctly authenticated, and legitimate emails sent via these new mail servers end up in the spam folder or are rejected by the mailbox provider.

SPF records frequently include too many IP addresses or entire network ranges, which can pose a security risk.

Domains that are not intended for email sending are often not protected against abuse but should also be equipped with an SPF record. *"v=spf1 -all"*

DKIM:
For DKIM, the generation of a public and private key pair for the domain is necessary, with the public key stored in the DNS entry. The private key is applied to sign each outgoing email. The receiving server then compares the private key with the public key.

Example:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=12dkim1;
d=emails.firma.com; h=From:To:Subject:Date:MIME-Version;
i=company@emails.company.com;
bh=LIHvJ+o6R8cJxg5BzQc0JiypsEb3u891LpwUMSgE6nY=;
b=dGh93t7sUgSqoyoBASeIdmnQuSM5iWU81wye+4tzVRpsQ5Tz4r7IvVVpnrfi+39+X
xx27bAvx6cXyPgp0GdRCLMCUi+72yAGEqQ5us755HLTgTbUjnTopHtv0r09TE1n9wKX
2iXAj8IBKJiC6oQg2GMRn3PgkyjrcR67S6UJmlHKcbjdxuv7JgBZr3PTOPWmDq9BrUU
eiAYrqO5mhGoT51GBi+btPkXYugkIQhL3/XhScf57InbxpMJsNAP1eXJG2viS989UAe
N+uvSv+rwR8EA2bhMhjdCqxcrNyo0t2MW3GJi1NuyAN6+ukQ9vgbYUfq3jJu6APkewj
hHFhQthbQ==
```

Common errors:

- Inadequate domain configuration, such as incorrect key lengths, faulty DNS entries and outdated DKIM keys, can enable cybercriminals to abuse the domain.
- Lack of key rotation.
- Insufficient signature scope, which only refers to individual email headers.
- The use of the length parameter (l=) limits the signature to a certain part of the email and leaves room for manipulation in the unsigned part of the email.
- The domain used for the DKIM signature is too general and often does not match or relate to the visible sending domain.

DMARC:
A DMARC record is created to define in the policy how emails that fail the SPF and DKIM checks should be handled by the receiving server. (Emails are denied with the "reject" policy, emails are delivered to the spam folder with the "quarantine" policy, or no specific action is taken with the "none" policy)

> **Example:**
> `v=DMARC1; p=quarantine; rua=mailto:example@company.com`
>
> This record uses the "quarantine" policy, and as per the instruction, non-authenticated emails are delivered to the spam folder. The "rua" tag here specifies where the daily available DMARC reports should be sent.
>
> **Challenge:**
> A common error in DMARC configuration is hastily setting a too strict policy without sufficient monitoring or analysis of the existing sending infrastructure. This can result in legitimate emails being blocked or filtered.
>
> A DMARC implementation must always be accompanied by monitoring of the DMARC reports. This is the only way to detect configuration errors or cases of abuse and take action to protect against them.

The implementation of SPF, DKIM and DMARC is often complex and requires in-depth knowledge of DNS and email security. It is recommended that you seek expert help if needed.

7. Access to real data & monitoring – a necessity for security and risk management

Access to performance data from sending servers, domains and email campaigns is essential to detect and address cyber threats and deliverability problems from an early stage. However, it is also one of the biggest challenges. Without this real data, cyber threats and issues may not be detected in time and addressed appropriately, but mailbox providers do not simply provide this information, and it can vary in form and manner from provider to provider.

Use of DMARC reports

The DMARC standard has been developed and introduced for the purpose of consistent reporting. It serves as an effective monitoring tool for the SPF and DKIM

authentication protocols. DMARC reports help senders quickly detect and respond to unauthorised domain abuse and security breaches. Regular analysis of these reports is crucial. These reports follow a standard format and are sent by an increasing number of mailbox providers. However, to analyse these reports, appropriate evaluation tools are required to make the technical reports readable for an end user.

Email performance monitoring

Continuous monitoring of email campaigns is crucial for a company's security and efficiency in order to:

- Ensure reliable delivery of emails to the inbox;
- Build and maintain a positive domain reputation;
- Identify proactively manage risks by identifying vulnerabilities at an early stage.

8. The CSA as a reliable partner for enhanced email security and quality

The Certified Senders Alliance (CSA) provides certified senders with comprehensive support in the form of uniform standards, which are developed in collaboration with mailbox providers, and which are regularly updated. These standards are used to monitor compliance with a high-performance monitoring tool. This tool is based on real data from mailbox and security providers, offering valuable insights into email authentication and email performance.

The correct application of authentication protocols is a core component of the CSA criteria, but, above all, it is the fundamental aspect of a company's email security.

The CSA Certification Monitor offers:

- Email performance data: to identify and resolve reputation and delivery issues from an early stage, caused for example by high spam click rates and spam trap hits;
- Authentication data: Identification of authentication gaps, such as DKIM errors.

Risk reduction through targeted advice from CSA experts:
Certified senders receive valuable, personalised feedback on non-compliant emails from deliverability and legal experts. This feedback helps to identify deficiencies and avoid potential damage, including:

- Notifications about user complaints;
- Forwarding serious complaints from mailbox providers;

- Information on legal requirements and technical irregularities;
- Expert advice and support for troubleshooting.

The CSA community and training opportunities:
The CSA brings email senders together with mailbox providers, promotes exchange and offers valuable interactions within the industry. Certified senders benefit from specialist knowledge and the sharing of experiences.

- CSA network: Exchange within the email community;
- Exclusive training opportunities: Discounts on webinars, training and workshops, tailored to the needs of members;
- CSA certificate: Recognised as a seal of quality for senders in the industry.

9. Conclusion – Email authentication is a MUST

Today, reliable email authentication is essential to maintaining customer trust, protecting corporate reputation and minimising financial risk. This is particularly crucial in the finance and insurance sectors, where it is essential to live up to the high level of trust that customers place in you and to continuously ensure their security actively. Companies must continuously adapt to the dynamic threat landscape and prioritise the improvement of their security measures to ensure that their emails also end up in their customers' inboxes.

Email authentication is therefore not an option, but an absolute must.

The Certified Senders Alliance offers certified senders continuous and valuable support in this regard.

10. Frequently asked questions

What does email deliverability mean?

Email deliverability refers to an email reaching the recipient's inbox without ending up in the spam folder or being rejected by the receiving mail server.

Who are mailbox providers?

Mailbox providers are companies that offer email services and enable the receipt, sending and storage of emails. They provide users with email addresses and ensure the security of email communication through complex filter technologies to prevent phishing and spam.

Who are some well-known mailbox providers?

Some of the most popular providers in Germany include:

- 1&1 (Web.de, GMX.de);
- Deutsche Telekom (T-Online);
- Google (gmail.com);
- Microsoft (outlook.com, hotmail.de,…..);
- Yahoo.

What key performance indicators (KPIs) are important in the field of email marketing?

- **Delivery rate:** The percentage of successfully delivered emails;
- **Deliverability rate:** The percentage of emails that reach the inbox;
- **Bounce rate:** The percentage of emails that are rejected due to delivery errors;
- **Complaint rate:** The percentage of emails marked as spam by recipients;
- **Open rate:** The percentage of emails that are opened;
- **Click-through rate:** The percentage of recipients who clicked on a link in the email;
- **Unsubscribe rate**: The percentage of recipients who clicked on the unsubscribe link in the opened email;
- **Conversion rate**: The percentage of recipients who performed a desired action.

These performance indicators are crucial for monitoring and optimising email performance, protecting the sender's reputation and increasing recipient engagement.

What is DNS and how is it used?

The Domain Name System (DNS) is the phonebook of the Internet. It is used to convert human-readable domain names, such as "brand.com", into computer-readable, numerical IP addresses, such as "192.0.2.1". Computers can use these addresses to locate and communicate with each other on the Internet.

Domain owners can access the DNS of their domain through their domain registrar's account and, if necessary, create or modify DNS records. These DNS records make it possible to precisely control and configure traffic for a domain by determining how and where requests for that domain are directed.

Each DNS record serves a specific function and is used to manage various aspects of domain name administration, such as:

- Linking an IP address to a domain name (A record);
- Defining the servers authorised to receive emails for the domain (MX record);
- Verifying domain ownership and providing additional information about the domain (TXT record);
- Specifying information about the domain's management service (NS record).

What is the difference between spoofing and phishing?

Spoofing: This is a technique used by cybercriminals to impersonate a legitimate or a well-known email sender, such as through domain abuse. The goal is to gain trust or conceal identities in order to prompt the recipient into interaction.

Phishing: This refers to the attempt to trick the recipient into disclosing personal or confidential information through fraudulent emails. The main objective is the theft of sensitive data through deception.

> **Example:**
> A fraudulent email from a bank prompts the recipient to click on a link that leads to a counterfeit login page. There, the recipient is asked to enter their login credentials, which are then stolen by the attacker.

What is a bounce?

A bounce, in the context of reputation or authentication issues, occurs when an email fails to be delivered due to doubts about the sender's legitimacy or lack of authentication. In such cases, the recipient's mail server refuses to accept the email because it cannot verify the sender's identity or because the sender has a poor reputation – for example, due to many user complaints or suspicions of spam or phishing. The sender receives a "Non-Delivery Report" (NDR) or a "bounce message" from the recipient's mail server, indicating the reason for the rejection using a bounce code. An increased bounce rate can further deteriorate the sender's reputation and lead to even more serious delivery issues.

About the Certified Senders Alliance

The Certified Senders Alliance (CSA) is a service from eco – Association of the Internet Industry in cooperation with the German Dialogmarketing Association (Deutscher Dialogmarketing Verband – DDV) and was created in 2004. The CSA acts as a neutral interface between mailbox providers and senders of commercial emails. The goal of the CSA is to increase the quality of commercial emails (e.g. newsletters, invoices, order confirmations, etc.). To achieve this goal, the CSA establishes legal and technical quality standards. The quality standards arise out of prevailing law and the technical requirements for mailbox providers. They are regularly updated to correspond to the current legislation and market requirements.

About the author

Sandra is an experienced email marketing and customer service professional. As an email marketing consultant at Validity/Return Path in France, she worked with brands to address deliverability issues and refine email strategies. Prior to that, she supported her clients in various roles in an international environment, including client success and channel support at Return Path and export management at Carl Zeiss. Since August 2023, she has returned to customer support in her home country Germany, where she combines her expertise and passion for helping others as Customer Support Manager at CSA.

Sandra Schubert
Customer Success Manager
Certified Senders Alliance

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 Cologne
Register of Associations Number: 14478
VAT-ID: DE 182676944