CCN-CERT

BP/33

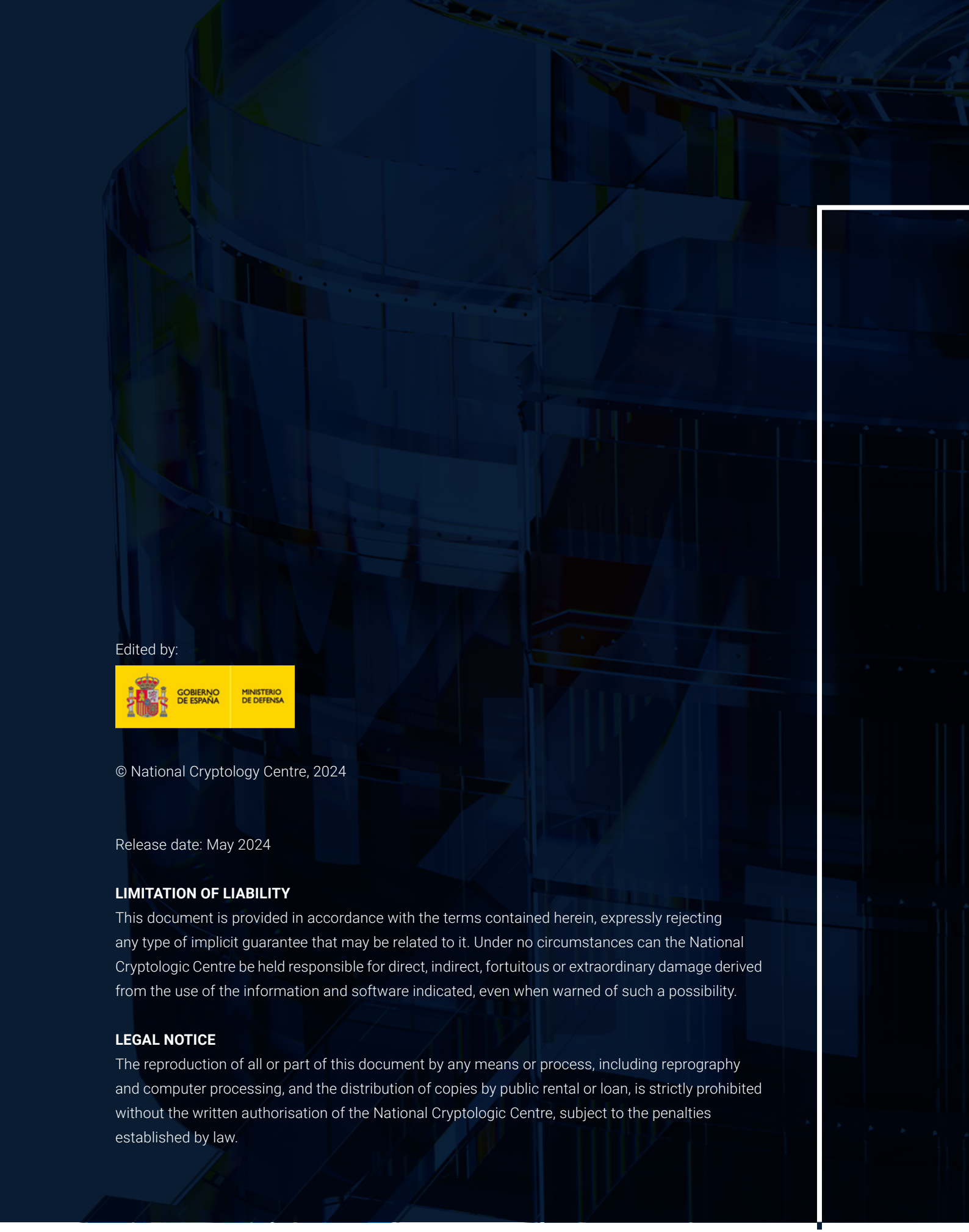
Best email security practices, DMARC

BEST PRACTICES REPORT

MAY 2024

ccn-cert centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional



Edited by:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Release date: May 2024

Index

1. Aim of the guide

The content of this document explains the concept of DMARC (Domain-based Message Authentication Reporting & Conformance), the protocol, the definitions, its practical applications and the implications of implementing it. In addition, it discusses in detail what DMARC is for, highlighting its benefits and how it contributes to strengthening the security and authentication of emails.

It also examines the implications of implementing DMARC, detailing how this measure can impact on the identification and prevention of phishing attempts and other email-related cyber-attacks.

It presents concrete examples of situations that may arise when implementing DMARC and provides essential information to understand how this tool contributes to ensuring the integrity and authenticity of electronic messages.

In summary, **this document is a comprehensive guide to DMARC,** providing a detailed overview of its purpose, usefulness and the practical consequences of its application.

The document describes the DMARC protocol and how it improves email authentication, prevents phishing and enhances security.

2. Introduction, DMARC and its importance

2.1. Introduction to DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email validation protocol designed to protect email domains from phishing and other forms of email abuse, such as fraud and phishing. Its history can be traced back to collaboration between several organisations and email security experts. It is specified in the **RFC7489**[1] standard.

DMARC has two main functions:

- Verify the authenticity of the e-mail.
- Prevent fake emails from reaching their destination.

Initial context

Before DMARC, there were already SPF (*Sender Policy Framework*)[2] and DKIM (*DomainKeys Identified Mail*)[3], which are methods for verifying whether emails come from legitimate sources. However, these methods had limitations, especially in how messages that failed these verifications were handled.

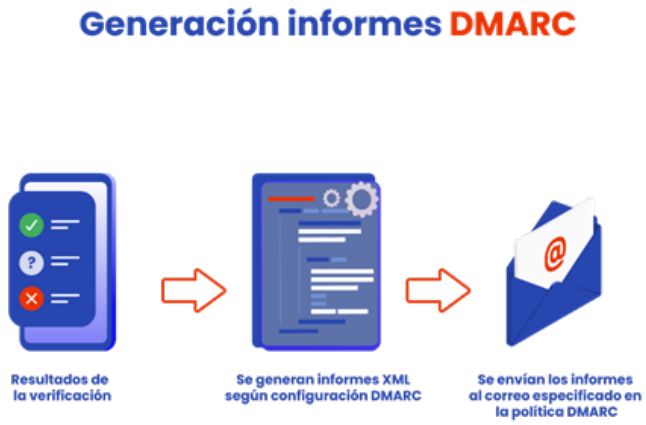
1: https://datatracker.ietf.org/doc/html/rfc7489
2: https://datatracker.ietf.org/doc/html/rfc7208
3:https://datatracker.ietf.org/doc/html/rfc6376

Need for a new standard

The protocol emerged as a solution to fill the gaps left by SPF and DKIM. It would allow domain owners to specify how to handle emails that would not pass individual **policy** checks, as well as build a standard **reporting** format with informational messages that receiving servers send to domain owners about the authenticity of received emails.

These reports help domain administrators understand how their emails are being treated in the outside world, including how many messages passed or failed SPF and DKIM checks, and how they were handled in accordance with established DMARC policy.

The reports are delivered in an XML format and provide detailed data that can be used to monitor and improve email security measures, **detect configuration problems, combat abuse and fraud, and understand the degree of alignment with DMARC.**



Collaboration and development

DMARC was developed in 2012 by a working group that included large technology and communications companies such as Google, Microsoft, Yahoo, AOL, and others. The idea was to create a standard that everyone in the industry could use to make email more secure and reliable.

2.2. Importance of DMARC for public institutions

The implementation of DMARC is crucial for public institutions for several reasons:

- **Anti-phishing email protection** prevents malicious actors from sending fraudulent emails that appear to come from legitimate domains of these Public Institutions.
- **Integrity of the information** ensures that the information sent by e-mail has not been altered.
- **Citizen confidence increases** trust in e-mail communications of public institutions.
- **Sovereignty,** in the context of today's geopolitics, protection against disinformation campaigns and cyber-attacks is more important than ever to preserve integrity and sovereignty.

The business of cybercrime has found domain and email spoofing to be a lucrative activity. Through phishing and social engineering techniques, these cybercriminal groups can gain access to sensitive information, manipulate political events, or even paralyse critical infrastructure.

A current public entity should work towards a 100% quarantine policy in a reasonable timeframe, depending on the declared and the steps below.

3. Technical considerations prior to DMARC implementation

3.1. What is SPF and how is it configured?

SPF allows domain owners to specify **which mail servers are authorised to send emails on behalf of their domain.** This is achieved by publishing an SPF record in the domain's DNS. Receiving mail servers can query this record to verify whether the mail they are receiving is coming from a server authorised by the sender's domain owner.

Example of SPF

Suppose an entity with domain "entity.com" wants to implement SPF to protect itself. The entity sets up an SPF policy that only allows mail to be sent from their internal mail servers and, optionally, from a mail service provider they use. The SPF record in the DNS for "entity.com" might look something like this.

```
v=spf1 ip4:192.168.0.1 include:mailservice.com -all
```

This SPF record indicates the following:

- **v=spf1,** The version of SPF being used.
- **ip4:** 192.168.0.1, emails sent from IP address 192.168.0.1 are allowed.

include: mailservice.com includes the SPF policy for the domain "mailservice.com", which is an example of an authorised external email service provider.

-all: A failure mechanism indicating that any server that does not meet the above criteria is not authorised to send mail from "entity.com".

When a receiving server receives an email claiming to be from "entity.com", it will check against the SPF record. If the mail comes from a server not listed or authorised in the SPF record, it will be rejected or marked as suspicious, depending on the configuration of the receiving server.

In the example we have only discussed the essential parameters: version, ipv4, include and all. This is the minimum necessary for SPF to work properly, assuming the rest of the defaults are adequate for most implementations. It is not common to see the rest of the parameters, but these are:

Label	Description and permitted values
v	This is always the first parameter in an SPF record and declares the SPF version being used. There are no alternatives to this value; it must always be **spf1**.
ip4 and ip6	These mechanisms specify **the IP addresses** (in IPv4 or IPv6 format, respectively) **that are authorised to** send mail on behalf of the domain. There is no default value for these fields; they must be explicitly configured with the correct IP addresses. ipv4 is a different label than ipv6, commonly only ipv4 is currently used.
include	This mechanism **allows you to include the SPF policy of another domain within your SPF record.** It is useful when using third party services to send emails on behalf of your domain. As with ip4 and ip6, there is no default value.
a and mx	These mechanisms **allow emails to be sent from the IP addresses associated with the A or MX records of the domain**, respectively. If used without additional parameters, they refer to the domain itself. There are no default values; they apply only if explicitly included.
ptr	**It is not recommended due to performance issues** and because it is not effective as a verification mechanism. The ptr mechanism verifies that the reverse IP address of the sender matches the specified domain.
exists	This mechanism allows the domain to **specify a DNS query** that, if it resolves, allows the IP to pass. It is rarely used due to its complexity and load on DNS servers.
redirect	Allows the **SPF assessment** to be **redirected** to another domain. If used, completely replaces the original domain's policy with that of the domain to which it is redirected.

The all mechanism

All is a mechanism that **specifies how emails that do not match any of the previous mechanisms in the SPF record should be treated.** It is the catch-all at the end of the record and is vital because it defines the default behaviour for IP addresses that are not specifically authorised. It should always appear at the end of the DNS record for the SPF:

all	Description
+all	Allow any server to send mail on behalf of your domain (this effectively **disables SPF as a security measure and is not recommended).**
-all	Indicates that mail sent from servers not specified in the SPF record should be rejected (Recommended).
~all	It results in a **"softfail" policy**, which suggests but does not require messages to be treated as spam or rejection; it is useful for the testing phase.
?all	Indicates a neutral policy where no instructions are given on how to deal with mails that do not match other registry mechanisms.

3.2. What is DKIM and how is it configured?

DKIM allows the sender's domain to associate its domain with an e-mail message by adding a digital signature to the message header. This digital signature is created using a private key that only the sender possesses, and any recipient can verify this signature using the corresponding public key, which is published in the DNS of the sender's domain.

Example of DKIM

Let's imagine that the entity "entity.com" wants to implement DKIM for its emails. The system administrator of "entity.com" generates a pair of cryptographic keys (one private and one public). The private key is used to digitally sign the domain's outgoing emails, while the public key is published in a DKIM record in the domain's DNS.

A possible DKIM record in the DNS of "entity.com" could look like this:

```
dkim._domainkey.example.com. IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC..."
```

This DKIM record indicates the following:

- **dkim._domainkey,** the standard prefix indicating where the DKIM public key for the domain "entity.com" is located.
- **v=DKIM1,** the version of DKIM.
- **k=rsa,** the type of cryptographic key used, in this case RSA.
- **p=MIGfMA...,** the public key used to verify digital signatures.

When a receiving server receives an e-mail claiming to be from "entity.com", it will verify the signature in the mail header using the public key. If the verification is successful, this confirms that the message really comes from "entity.com" and that it has not been modified in transit. If the verification fails, the mail may be treated as suspicious.

In the example we have only discussed the essential parameters: version, key type, and the public key. This is the minimum necessary for DKIM to work properly, assuming the rest of the defaults are adequate for most implementations. It is not common to see the rest of the parameters, but these are:

Label	Description and permitted values
v	DKIM version, default: **DKIM1**. This parameter must always be present and set to indicate that this is a DKIM record.
h	Allowed hashing algorithms. Generally, it is not specified and systems assume the most common ones such as **sha256.**
k	Key type, DKIM uses **rsa** by default, and is the most commonly used key type for signing emails.
p	Public key, this field must contain the public key which corresponds to the private key used to sign e-mails.
s	The scope of the emails that the signature is intended to cover is generally not specified and ***** is assumed, meaning that the signature is valid for **all emails in the domain.**
t	Signature timestamp, not commonly used in DKIM records, time validity management is done in the software verifying the signature.

Label	Description and permitted values
g	Signature granularity. Defines which specific users the signature applies to. By default, it is usually set to match any user (*****).
n	Notes, free text field to include administrator comments.
o	Signature policy, indicates whether all mails must be signed (-) or whether some mails may not be signed (~).
i	Identity of the user signing the message. This allows you to specify a particular e-mail address in the "From:" field that the key is supposed to sign.

3.3. What is DMARC and how is it implemented?

DMARC uses the aforementioned SPF and DKIM technologies to verify that e-mail messages originating from a domain are authentic and have not been altered in transit.

In addition, it allows domain owners to set policies that dictate how receiving servers should handle mail that fails these checks. It also provides a reporting system that allows domain administrators to receive feedback on the performance of emails sent from their domain and how they are being processed under DMARC policies.

Example of DMARC

We continue with the example of the entity "entity.com" and it wants to implement DMARC to improve the security of its email. The system administrator of "entity.com" adds a DMARC record to the DNS of the domain, which could look like this:

```
v=DMARC1; p=none; rua=mailto:reportes@proveedordmarc.com;
ruf=mailto:fallos@proveedordmarc.com; fo=1; adkim=r; aspf=r
```

This DMARC record indicates the following:

- **v=DMARC1:** Version of DMARC.
- **p=none:** DMARC policy that asks not to take any action on mails that do not pass SPF and/or DKIM tests, but to generate reports.
- **rua=mailto:**reportes@proveedordmarc.com, email address to receive aggregated authentication reports.
- **ruf=mailto:**fallos@proveedordmarc.com, email address to receive detailed forensic reports of authentication failures.
- **fo=1:** Generate failure reports if any check (SPF or DKIM) fails.
- **adkim=r; aspf=r,** relaxed alignment for DKIM and SPF respectively, indicating that the domain part must match the domain in the message, but allows for some discrepancies.

By using this DMARC record, "entity.com" does not protect its brand from misuse in email by the selected policy but allows it to receive valuable information about the performance and security of its email communications, allowing it to make continuous adjustments and improvements to its security protocols in order to plan a policy change.

In the example we have only dealt with the basic parameters: version, policy, rua, ruf and fo. This is the minimum necessary for DKIM to work properly, assuming the rest of the default values are adequate for most implementations. It is not common to see the rest of the parameters, but these are:

Label	Description and permitted values
v	DMARC protocol version, currently DMARC1.
p	Policy to apply to e-mail that do not pass DMARC verification. It can be: ◆ **none:** This policy allows all emails to reach their destination, even if they fail DMARC verification. It is used as a monitoring policy to analyse failure reports and determine the level of DMARC alignment. ◆ **quarantine:** This policy determines that emails that fail verification are marked as *spam*. ◆ **reject:** This is the strictest policy, whereby emails that fail verification are rejected and prevented from reaching their destination.

Label	Description and permitted values
sp	Policy to apply to e-mail, corresponding to **subdomains**, which do not pass DMARC verification. If this tag is omitted, the policy defined in the "p" tag shall apply to subdomains.
aspf	The *aspf* alignment mode refers to the accuracy with which the sender records are compared with the SPF signatures, with two possible values: ◆ "r" (**relaxed**) allows partial matches, such as sub-domains of a given domain. ◆ "s" (**strict**) requires an exact match.
adkim	The *adkim* alignment mode refers to the accuracy with which sender records are compared with DKIM signatures, with two possible values: ◆ "r" (**relaxed**) allows partial matches, such as sub-domains of a given domain. ◆ "s" (**strict**) requires an exact match.
pct	The percentage tag indicates that they only apply the DMARC policy to a **percentage** of the failed emails. "pct=50" will instruct receivers to only apply the policy to 50% of the emails that fail DMARC verification. If this tag is omitted, it will be applied to 100% of failed emails. The pct tag was designed to gradually apply DMARC policies to shorten the implementation period for online businesses.
rua	List of URIs for sending **aggregated** feedback XML **reports**. RUA reports are aggregated summaries that receiving servers send to a domain owner to report on the volume and authentication results of emails sent on their behalf. DMARC requires a URI or list of URIs and not just an email, remaining: "mailto:analizador-dmarc@receptor-del-reporte.com".
ruf	List of URIs to send **forensic reports**. RUF reports are messages that receiving mail servers send to a domain owner to provide detailed information about individual incidents of message authentication failure. Currently disused by most mail providers as there are privacy issues with communications. DMARC requires a URI or list of URIs and not just an email, remaining: "mailto:analizador-dmarc-forense@receptor-del-reporte.com".
rf	Failure Reporting **Format**. This can be either "afrf" (Authentication Failure Reporting Formats) or "iodef" (Incident Object Description Exchange Format). By default, its value is "afrf".
fo	Tag used within the DMARC register to specify the **conditions** under which receivers shall **generate and send** fault reports. Allowed values are: ◆ "0" to generate reports if both DKIM and SPF fail ◆ "1" to generate reports if DKIM or SPF fails ◆ "d" to generate a report if DKIM fails ◆ "s" to generate a report if SPF fails This field can have multiple combined options.
ri	Interval between reports expressed in seconds. This is the frequency with which you wish to receive aggregated XML reports. This is a preference, providers must have the ability to provide a daily report, but if the interval is less, the best effort basis applies. By default, its value is "86400".

3.4. DMARC alignment

The SPF and DKIM security mechanisms are sufficient to validate that an email is sent from an authorised server, but they do not guarantee, in any case, that they are not being impersonated. To avoid this situation, DMARC incorporates a new security concept called "DMARC Alignment".

To understand this concept, it is essential to understand the differences between the "Mail From" and "Header From" headers and their importance in the DMARC alignment process. The "Mail From" is used during the authentication process (DKIM and SPF are applied to it) and the "Header From" is used during mail display. In other words, a server may authenticate correctly, but may use a spoofed identity as the sender, which will appear to the user during display. Therefore, it is the DMARC alignment that will prevent a server, legitimately authenticated, from sending mails using unauthorised domains as sender.

Importance of Mail From, Header From, SPF and DMARC in the DMARC alignment

In the DMARC alignment process, both the "Mail From" and the "Header From" are examined and the results of the SPF and DKIM checks are considered. Two separate alignment checks are performed:

- **SPF aligned:** For SPF alignment to occur, it is necessary that the mail complies with the SPF check and that the "Mail From" and "Header From" belong to the same domain.

- **DKIM aligned:** For DKIM alignment to occur, it is necessary that the mail complies with DKIM verification and that the domain used during DKIM integrity signing belongs to the same domain as the "Header From" user.

If one of them is met, an e-mail is partially aligned, and if both are met, it is considered to be fully aligned. Only one of them needs to be met for it to comply with DMARC correctly.

Relaxed and strict alignment

In DMARC, SPF and DKIM alignment can be relaxed or strict. In relaxed mode, a match is allowed by accepting subdomains between the "Header From" header and the domains parsed by SPF and DKIM while, in strict mode, an exact match is required.

The following table shows when each type of alignment is fulfilled depending on the domains of the "Header From" and "Mail From".

Header From	Mail From	Relaxed alignment	Strict alignment
example.com	**example.com**	Complies	Complies
app.example.com	**app.example.com**	Complies	Complies
example.com	**app.example.com**	Complies	Non-compliant
app.example.com	**example.com**	Complies	Non-compliant
app.example.com	**email.example.com**	Complies	Non-compliant
example.com	**badmail.com**	Non-compliant	Non-compliant

3.5. How to create an SPF, DKIM and DMARC TXT record

To create a DNS record, including a DMARC record, you can follow these general steps that apply to most DNS service providers. The steps are detailed here without including specific examples:

Access to the DNS manager
Log in to the control panel of your hosting provider or domain registrar where your DNS is hosted.

Locate the DNS or Domain management section in your control panel.

Navigate to DNS records management
Go to the specific section where you can view and modify DNS records.

This might be labelled "DNS Zone", "DNS Manager", "DNS Settings", or something similar.

Add a new record
Select the option to add a new record. This may be a button or link that says "Add Record", "New Record", or "Create Record".

Specify the type of registration and details
Choose the appropriate record type, you will select "TXT" as the record type.

Specify the host name or record name.

- **For an SPF record** generally, the hostname for an SPF record is simply "@" if you want it to apply to the primary domain.

  The SPF record value must start with v=spf1 followed by the directives specifying which servers are allowed to send mail on behalf of your domain.

- **For a DKIM record** the hostname is usually something like selector._domainkey. Here, "selector" is a prefix that can be defined (it is a label that helps identify the specific key used to sign mail). For example, if you choose mail as the selector, the full record name would be mail._domainkey.yourdomain.com.

  The value for a DKIM record includes the DKIM version (v=DKIM1), the key type, and the public key itself.

- **For a DMARC record,** usually type "_dmarc". This will make the full name of the record "_dmarc.entity.com".

  Enter the registry value. This is where you will place the details of the DMARC registry, such as policy, email addresses for reporting, etc.

Save the record
Check the information you have entered to make sure it is correct.

Save or apply the changes. There may be a button that says "Save", "Apply", or "Update".

Verification
Verify that the registry has been created correctly using local tools such as the "dig" command or via third party online tools such as MXToolbox or similar, to ensure that the registry is propagating and publicly accessible.

Wait for propagation
Note that changes to DNS records can take time to propagate. This time can vary from a few minutes to 48 hours, depending on the TTL (time to live) configured for the records and the DNS provider.

3.6. Proper use of DKIM selectors

A selector in DKIM is a string of characters that uniquely identifies a specific set of public keys used to sign email messages using DKIM. Each domain implementing DKIM can have multiple selectors, each associated with a unique public/private key pair. The selector is included in the DKIM header of the signed email, allowing the receiving server to identify which set of keys to use to verify the DKIM signature.

One of the best practices in the use of DKIM selectors is to use multiple selectors for different sets of keys, which facilitates the management and revocation if necessary. This involves assigning a specific selector for internal mail servers and creating separate selectors for each third party or external service that sends mail on behalf of the organisation. By doing so, a compromised set of keys can be selectively revoked without affecting the authentication of other services. In addition, it provides greater granularity in key management and improves the overall security of the DKIM system.

3.7. Additional measures during the implementation of DMARC policies

During the implementation of DMARC policies, it is critical to consider additional measures to strengthen email security and mitigate the risks of phishing and phishing. In addition to "reject" or "quarantine" policies, for emails that do not comply with SPF, DKIM or DMARC, there are other actions that organisations can take to protect their users:

- Replacement of the "Header From" by the "Envelope From" when DMARC is not complied with, allowing the actual sender to be displayed instead of the "Header From" which could be spoofed.
- Add an information banner that alerts the user to the possibility of phishing and advises caution when opening the mail.

These controls are applied during the reception of emails from users of the protected domain. These measures are not very intrusive but are effective in alerting users to suspicious emails. It is important to note that these controls do not in any case prevent the impersonation of domain users to a third party (this is done thanks to SPF, DKIM and DMARC) as they operate on the infrastructure of the domain we are protecting.

4. Planning and preparation

4.1. Analysis of the e-mail infrastructure

Before implementing DMARC, it is essential to conduct a full audit of the current email infrastructure. This includes:

- **Identify all email domains that need DMARC protection.** This includes primary domains, subdomains and any other domains used to send legitimate emails.
- **Conduct a complete inventory** of all systems that send emails on behalf of your domain, including internal systems and external providers.
- **Review the existing SPF and DKIM records** for each domain. Ensure that these records are correctly configured and aligned with the email services used.
- In case of using Institution-owned mail servers, **assess the hardware and software used** to verify that they are up to date and that best security practices are applied.
- Consider applying DMARC to **domains that are not used** for email to prevent spoofing by malicious actors.

4.2. SPF and DKIM configuration

Before setting up DMARC, the correct implementation of the SPF and DKIM standards must be ensured.

- **Review or configure SPF and DKIM records** to ensure that they are correctly aligned with the email services used to send mail on behalf of the domain.
- Ensure that all mail servers authorised to send mail are **listed in the SPF record.** If necessary, a complete listing should be requested from the email service providers being used.
- Ensure that the email infrastructure is capable of generating **valid DKIM signatures** and that inclusion in the DNS record is allowed.

4.3. Determining the initial DMARC configuration

The initial implementation of DMARC should include at least the following points:

- Define **what you hope to achieve with DMARC** not on the basis of the current state of alignment, but on the basis of the ultimate or ideal goal. With this we have a target policy.
- Ensure that **IT and security teams understand how DMARC** and its dependencies with SPF and DKIM **work**.
- **Decide the initial DMARC policy** for each domain. The policy can be *"none"*, "*quarantine*" or "*reject*" for emails that fail SPF and DKIM authentication.
- In case you have nothing configured or doubts about the alignment, **publish a DMARC record with a policy of none** (p=none) to monitor and not affect the existing mail flow.
- **Include in the registry the addresses for the** aggregated **reports** (rua) to receive the analysis of the mails that pass and fail the checks.

4.4. Establishment of a protocol for continuous monitoring and adjustment of the DMARC policy

The implementation of DMARC is not a single event, but a continuous, step-by-step process that requires continuous monitoring, analysis of results and adjustments to the DMARC configuration.

- **Establish at least one specific email address** to receive DMARC reports for further analysis. It is recommended to work with companies that analyse and manage the data for easy reading of the data in graphs and metrics.
- **Set up a security team** that is responsible for the analysis of aggregated reports and the interpretation of such graphs from suppliers and can act accordingly.
- **Use third-party DMARC analysis tools** to assess the effectiveness of the policy and make adjustments.
- **Establish a process to regularly review** the status of DMARC, its alignment and understand emerging trends or issues.
- **Periodically review security policies** to ensure that they remain effective and relevant.
- **Identify legitimate email flows that are not aligned** with the current SPF and DKIM settings.
- **Adjust SPF, DKIM and DMARC settings** periodically as necessary to maintain a robust security posture. Based on the above points.

4.5. Establishing a change management protocol or process

The implementation of changes to the email infrastructure must be done in a controlled and documented manner. This involves:

- Develop an **implementation plan including milestones and timelines.**
- **Clear approval processes** for any changes to email settings.
- **Detailed records of changes made** to facilitate auditing and problem tracking.

4.6. Incident response and escalation procedure planning

Having a clear plan to respond to the problems identified by DMARC is crucial.

- **Establish clear communication channels** for reporting and responding to email-related security incidents.
- **Define a clear escalation procedure** for cases of attempted spoofing or significant abuse of the email domain that are detected.
- **Develop procedures for rapid investigation** of DMARC authentication failures.
- **Establish an incident response plan** that includes notification of affected users, correction of misconfigured DNS records and communication with authorities if necessary.

- **Regularly analyse DMARC reports** to detect and respond to emerging trends or new attack vectors. It is advisable to have a company assist in this process by representing the data with graphs and metrics.
- **Integrate DMARC reports with security analysis tools** to gain a deeper understanding of attack patterns and potential vulnerabilities.

4.7. Test planning and periodic validation

- **Conduct periodic tests** to validate the effectiveness of contingency plans and to check the state of updating and effectiveness of response procedures.
- **Include false positive drills** as part of regular incident response training to assess team preparedness and effectiveness of protocols.

4.8. Documentation and registration

- **Create standard operating guidelines** for the management and maintenance of DMARCs. Documentation is vital for sustainability and management.
- **Maintain detailed documentation** and audit trails of all DMARC, SPF and DKIM related actions and decisions to facilitate compliance with relevant regulations and incident investigations.
- **Maintain a detailed record** of all changes made and false positives identified and actions taken to resolve them.
- **Record and document all security incidents** and actions taken in response.
- **Use the information gathered to determine improvements** in email security policies and processes.

4.9. Training and awareness raising

It is critical that **technical staff involved in email implementation and management** understand the importance of email authentication and how DMARC can help protect against phishing and spoofing. This may include:

- **Workshops and webinars** on the basics of DMARC, SPF and DKIM.
- **Creation of quick reference materials** and guides for technical staff.
- **Continuous training** programmes to keep staff up to date with changes in regulations and technologies.
- **Establish communication channels** for users to report any problems related to the delivery of e-mails.

4.10. Coordination with e-mail providers

- **Work with email service providers** to resolve issues related to SPF and DKIM settings.
- **Establish service level agreements (SLAs)** with providers to ensure quick and effective responses when problems arise with legitimate emails.

5. Initial implementation from scratch

At this point, we are going to **exemplify** a situation in which the entity **has not created any registers**, has never implemented DMARC or wants to eliminate the current ones in order to create a solid documented base from which to build its process.

We are going to detail everything planned, starting with the exemplified configurations described and explained in **section 3.1.** of this document, **creating the SPF record with the data of all the providers and/or third parties authorised by the entity** to send e-mails on its behalf. Likewise, the configuration of DKIM, also described in **section 3.2.**, requires the communication or support consultation with the e-mail provider if this is not managed by the entity. Remember again that **DKIM must be implemented by all the e-mail providers**, they can share different TXT records to accept the signature of all of them in the case of multiple providers, the data of the record and content of the record must be provided by each of the providers

We would have something similar to these DNS records as an example:

```
@ IN TXT "v=spf1 ip4:192.168.0.1
include:emailprovider.com -all"

dkim._domainkey.entity.com. IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC..."
```

It is important to note that the doubts raised in this point should be resolved in sections 3.1. and 3.2.

5.1. DMARC's initial policy

- It is recommended to always set up an initial DMARC implementation, if one is not already in place, in monitoring mode (policy *none*) initially, to assess both the level of alignment and the possible impact on legitimate email delivery and spoofing attempts.

- Configure DMARC logs to generate aggregate and failure reports (*rua* tags) to be sent to a designated analyst or a third party offering DMARC analysis services.

As we have seen in **section 3.3.** of this document, the initial configuration for entities that did not have a DMARC registry or an entity that does not know its status.

Record Type TXT
Host Name _dmarc.entity.com
Registry Value

```
_dmarc.entity.com. IN TXT "v=DMARC1; p=none;
rua=mailto:reportes@proveedordmarc.com;"
```

Description of the Registry Components

- **v=DMARC1,** this specifies the version of the DMARC protocol being used.

- **p=none,** this policy indicates that while emails will be checked to see if they pass DMARC tests, no specific action will be taken if they fail. Essentially, this allows domain owners to monitor the effectiveness of SPF and DKIM without affecting the deliverability of their emails.

- **rua=mailto:reportes@proveedordmarc.com,** this part of the log indicates where the aggregate reports should be sent. Aggregate reports contain data on all sending attempts from the domain, which helps administrators understand how their mail is being handled in the network.

Using this record, servers receiving mail from your domain will not take punitive action against mail that fails DMARC tests, but will send aggregate reports to the specified address, allowing you to analyse and adjust your SPF and DKIM settings to improve the authentication of your mail. This is ideal for an initial phase of DMARC implementation, where you are still evaluating and refining your mail authentication policies.

5.2. Monitoring and gradual adjustment

- **Monitor DMARC reports** to identify email servers sending emails on behalf of the domain.
- **Develop a schedule** for reviewing alignment levels with a periodicity ($\mathbf{T_e}$)* established according to the type of institution.
- **Set clear thresholds** for each increment based on analysis of DMARC reports and user feedback: if it exceeds 95%, consider a policy change. This should start with a low percentage ($\mathbf{P_0}$)* and gradually increase ($\mathbf{P_{in}}$)* as confidence in the configuration is gained and the incidence of false positives is reduced.
- **Communicate changes to the DMARC policy** to all users so that they are prepared for possible questions or reports of legitimate mail being incorrectly flagged. Although the establishment of percentages for the gradual implementation of the policy is used to avoid false positives, it is possible that false positives may occur, and it is necessary for users to corroborate that no legitimate mail has been marked as unwanted.

5.3. Correction of problems

- **Identify and correct** SPF and DKIM **authentication problems** using DMARC reports. This may include adding new email services to SPF records, correctly configuring DKIM signatures, or addressing alignment issues.
- **Update SPF and DKIM records as necessary** to reflect changes in the email infrastructure.

4: * See section 7.

5.4. Review of reports

- **Analyse DMARC reports** to determine what percentage of emails are successfully authenticated and which emails fail authentication.
- **Identify any patterns of suspicious behaviour** or unauthorised activity that may require further action.
- **Use of third-party tools to obtain graphs, summaries, intelligence, metrics** and support based on the entity's specific data at the time.

6. Progressive implementation and refinement

6.1. Strategies for policy scaling up

Develop a schedule for reviewing and increasing the proportion of mail sent to quarantine. For example, you can start with a low percentage (**P_0**)* and gradually increase it (**P_{in}**)* if DMARC alignment levels are maintained or improved and the incidence of false positives is reduced.

Monitor the impact of the current policy on legitimate mail flows and perform validation tests to ensure that legitimate mail is not flagged as suspicious or blocked.

Adjust the configuration[3] of SPF and DKIM records based on the findings of the reviews to improve the level of alignment of DMARC.

6.2. Preparing for stricter policies

Once the maximum level (100% implementation rate) of the established policy has been reached and if alignment levels remain above 95% (if the policy is none) or 98% (if the policy is *quarantine*), a stricter policy can be considered. The same strategy specified above should be applied: start with a low percentage and gradually increase it.

5: * See section 7

6.3. Continuous monitoring

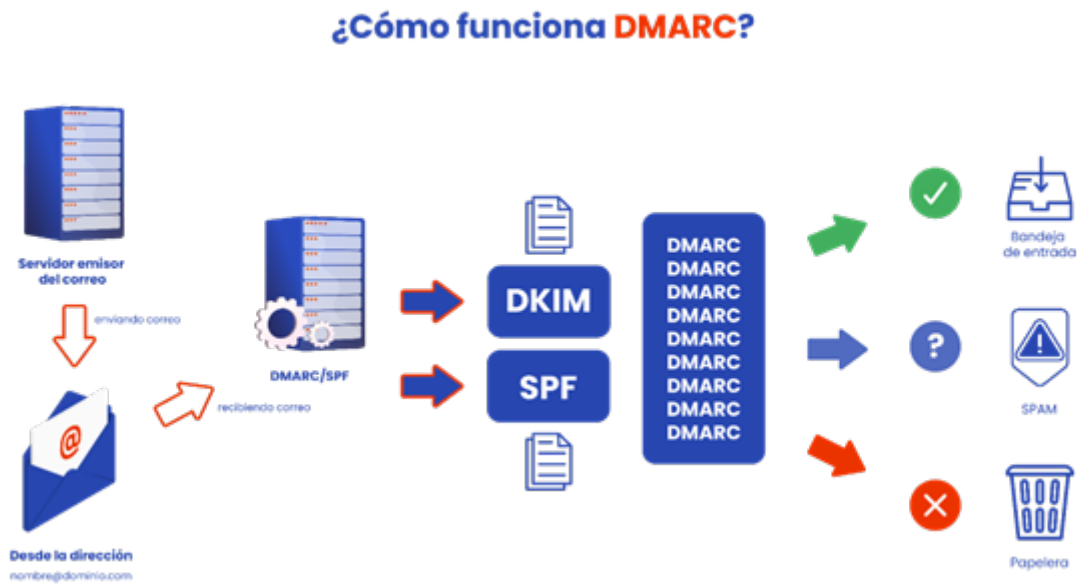
- **Continue to monitor** DMARC reports to identify any changes in email behaviour.
- **Take corrective action** as necessary to address any new issues that arise with email authentication.

6.4. Updating and maintenance

- **Maintain updated SPF and DKIM records** as necessary to reflect changes in the email infrastructure.
- **Conduct regular audits of DMARC configuration** and email authentication to ensure its continued effectiveness.

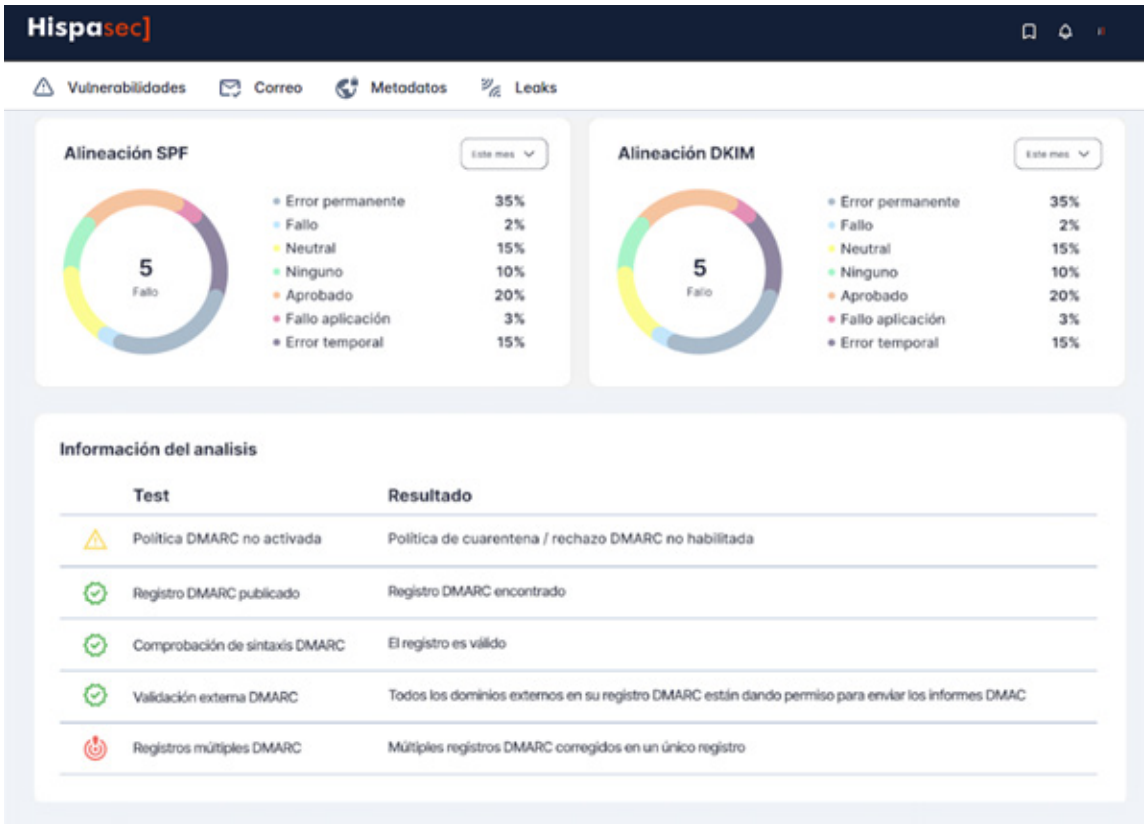
7. Implementation, consideration by volume of suppliers and size of the entity

At this point we want to see how it is implemented with steps, numbers and examples of implementation. A quick reminder at this point is that we have to keep in mind that the starting point is the "none" policy. Once we have aligned all providers, configured the SPF and DKIM correctly, we introduce the "quarantine" policy. This sends unaligned mail to spam, after a successful implementation of this policy, we can consider the next step, always taking into account the associated risks and move to a "reject" policy. This will cause the unaligned mail to disappear in the destination mailbox, not even being visible in the spam folder.



7.1. Identification of important data and metrics to assess and what might be considered good indicators for moving forward

In this section we will discuss effective tuning of a DMARC implementation and make informed decisions on how to move forward with SPF and DKIM policies. In this process it is essential to analyse alignment and performance data in detail.



7.1.1. SPF and DKIM alignment rate

The percentage of mails that pass SPF and DKIM checks should be observed. Ideally, this percentage should ideally be 100%, but in practice, **a percentage above 95%** is generally acceptable to consider that policies are working well.

The most common case in entities facing this process for the first time, due to ease of implementation, is to have SPF well aligned (section 3.1.) and to have some problems with DKIM implementation (section 3.2.). **If we observe that the DKIM alignment rate is low, it is crucial to reinforce the SPF configuration to ensure a high compliance rate in this area.**

A robust SPF can partially compensate for the weaknesses of DKIM, especially in the context of DMARC, where both mechanisms contribute to the overall compliance rate.

To improve the effectiveness of SPF in this scenario, an important measure to consider is to adjust the adkim directive in the DMARC registry. This directive controls DKIM alignment, setting **adkim=s (strict alignment) could be counterproductive if DKIM alignment is low,** so setting it to adkim=r (relaxed alignment) may be more beneficial. This means that only the domain part of the DKIM signature is required to match the domain part in the "From:" field of the mail header, rather than an exact match.

This change may help improve the rate of mails passing DMARC, allowing more flexibility in DKIM validation while relying more on the robustness of SPF.

This casuistry can be applied in the other direction, if DKIM is easy to implement, but SPF is not due to provider problems, in this case the parameter to avoid would be aspf=s.

7.1.2. DMARC alignment rate

It is crucial to measure the percentage of emails that are fully DMARC compliant, meaning that both SPF and DKIM are correctly aligned and pass the checks.

As with SPF and DKIM, **a DMARC compliance rate above 95% is a good indicator** that things are going well. This scenario is not always easy to achieve.

There is one very important and most common alignment for entities new to this process, and that is **partial alignment.**

This is the term used to describe a situation where only one of the methods, SPF or DKIM, is well aligned with the "From" domain, while the other is not. This is what could be happening:

- **SPF has a high level of alignment, but DKIM does not.** This means that the emails pass SPF verification correctly, and the domain used in SPF matches or is related to the domain. However, the DKIM signature may be failing or not aligned correctly.

- **DKIM has a high level of alignment, but SPF does not.** In this case, the DKIM signature is valid and the domain signing the message is correctly aligned with the domain, but the SPF check is failing, either because the mails are not coming from the servers listed in the SPF record or because the SPF domain does not match the "From".

This percentage of relaxed alignment does not give the data on how many of the mailings pass at least one of the validations, and between the two parameters to be measured, it is possible to have a very high percentage of partial alignment, above 90% or 95%. This is not ideal, but it is an important measurement when one of the implementations is not progressing at the desired or necessary level. This percentage does not carry the weight of alignment explained above, but it does carry weight in measuring the health and progress of the implementation.

This process of measuring relaxed alignment allows for greater flexibility. Mail sent from subdomains or with subdomain signatures can pass the DMARC check more easily. This is particularly useful for large organisations with multiple work units or external services sending mails on their behalf.

We cannot neglect the process of reviewing failure reports and aggregate reports to identify failure patterns, common error types, and problematic sending sources. These measurements should consider data such as frequency of failures, recurring problematic delivery sources, and specific types of configuration or alignment errors.

7.1.3 Considerations for moving forward with DMARC policies

- **Before making any changes to DMARC policy,** be sure to thoroughly analyse DMARC reports. Identify the causes of failures and address them before moving to more restrictive policies.
- **Gradual implementation,** if data indicates high compliance and alignment, consider moving the DMARC policy from none to quarantine. Start with a small percentage, such as a pct=10, and gradually increase if results are positive.
- **Communication with mail providers,** if you work with third parties to send mail on your behalf, make sure they are aware of your DMARC policies and that their systems are configured to comply with your SPF and DKIM requirements.
- **Ongoing education and testing,** continue to educate your team on DMARC, SPF and DKIM best practices. Conduct regular testing to ensure configurations remain effective as network infrastructures and email sending patterns change.

By following these steps and maintaining constant monitoring of DMARC, SPF and DKIM alignment data, you can safely move towards a more restrictive DMARC policy, which will improve email security and protection against fraud and phishing.

For this process, it is highly recommended to have a provider of metrics, graphs and all aggregated reporting information that originally comes in XML format represented in graphs. The ability to convert raw data into graphs and visualisations is essential for fast and effective analysis. To know these percentages of DMARC alignment, partial alignment, SPF alignment, DKIM alignment and their evolution over time. In addition, these platforms also allow you to discover at a glance the list of the faultiest providers in each of the categories, and even perform an in-depth analysis with ease.

7. Implementation, consideration by volume of suppliers and size of the entity

Visualisations can highlight trends, spikes in spoofing attempts, and other critical events that may require immediate attention. This is particularly useful during security reviews and presentations to management, where visual representations can be much more impactful than raw numbers.

A good provider will offer tools for **continuous monitoring,** enabling organisations to react quickly to new risks and threats as they emerge. This is essential in a constantly evolving threat landscape, where the ability to adapt quickly can mean the difference between a minor incident and a significant security breach.

In addition to organising and visualising data, providers can **offer actionable reports** that highlight specific problems and suggest corrective actions. This can include recommendations for SPF or DKIM record reconfiguration, DMARC policy adjustments, or even alerts on abnormal sending behaviour that could indicate a compromised account.

Businesses often need to **demonstrate compliance** with various security and privacy regulations. A provider that can generate detailed and accurate reports is invaluable in simplifying audit processes and ensuring that security policies comply with applicable regulations.

Choosing a provider that can offer advanced data organisation, analysis and visualisation services related to DMARC, SPF and DKIM is essential for organisations looking to optimise their email security and ensure the integrity and reliability of their communications.

7.2. Small entities or entities with 5 or less different e-mail providers

For entities with 5 or less different mail providers and other public entities of similar size, the implementation of DMARC may seem a simpler task given the number of providers. It is essential to protect both your communication and that of your citizens. The recommended levels are detailed here:

- **Check the alignment levels with a periodicity (T_e) of 60-90 days.**
- **Initial percentage (P_0) for quarantine or *reject* policies: 10%.**
- **Percentage rate of increase (P_{in}) for *quarantine* or *reject* policies: +10%.**

We must always work with **section 3.3.** as a reference, leaving an example configuration:

```
_dmarc.entity.com. IN TXT "v=DMARC1; p=quarantine; pct=30; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;
```

That, following a favourable review, it is decided to move forward to:

```
_dmarc.entity.com. IN TXT "v=DMARC1; p=quarantine; pct=40; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

After a further favourable review, it is decided to move forward to:

```
_dmarc.entity.com. IN TXT "v=DMARC1; p=quarantine; pct=50; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

And so on and so forth as long as the results are favourable and we do not detect any loss of mail.

7.3. Entities with more than 5 suppliers, of medium importance[6]

Entities of medium size or more than 5 email providers have a substantial responsibility to protect information due to the amount of sensitive data they handle and its potential impact on a larger population. The recommended levels are detailed here:

- **Check the alignment levels with a periodicity (T_e) of 45-60 days.**
- **Initial percentage (P_0) for *quarantine* or *reject* policies: 5%.**
- **Percentage rate of increase (P_{in}) for *quarantine* or *reject* policies: +5%.**

We must always work with **section 3.3.** as a reference, leaving an example configuration:

```
_dmarc.entity.com. IN TXT "v=DMARC1; p=quarantine; pct=30; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

6: Municipalities of between 100,000 and 1,000,000 inhabitants, Provincial Councils, Hospitals and Health Centers, Universities, Councils and medium-sized Public Entities.

That, following a favourable review, it is decided to move forward to:

```
_dmarc.entity.com. IN TXT "v=DMARC1; p=quarantine; pct=35; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

Following a further favourable review, it is decided to move forward to:

```
_dmarc.entity.com. IN TXT "v=DMARC1; p=quarantine; pct=40; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

And so on and so forth as long as the results are favourable and we do not detect any loss of mail.

7.4. Critical Entities [7]

Critical entities manage highly sensitive data and provide essential services that, if compromised, could have serious consequences for national security and public welfare. For this reason, the adoption of DMARC must be particularly rigorous and methodical, aiming for alignment with the most stringent policies. The recommended levels are detailed here:

- **Check the alignment levels at a periodicity (T_e) of 30-45 days.**
- **Initial percentage (P_0) for *quarantine* or *reject* policies: 2%.**
- **Percentage rate of increase (P_{in}) for *quarantine* or *reject* policies: +2%.**

We must always work with **section 3.3.** as a reference, leaving an example configuration:

```
_dmarc.entity.com. IN TXT "v=DMARC1; p=quarantine; pct=30; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

7: Ministries, Autonomous Communities, Army and State Security Forces, Critical Infrastructures.

7. Implementation, consideration by volume of suppliers and size of the entity

That, following a favourable review, it is decided to move forward to:

```
_dmarc.entity.com. IN TXT "v=DMARC1; p=quarantine; pct=32; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

After a further favourable review, it is decided to move forward to:

```
_dmarc.entity.com. IN TXT "v=DMARC1; p=quarantine; pct=34; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

And so on and so forth as long as the results are favourable and we do not detect any loss of mail.

8. Implementation implications

8.1. What DMARC does not do

It does not encrypt emails, DMARC does not provide any encryption mechanism for emails. Its function is to authenticate the source of the email and ensure that it has not been tampered with in transit, not to keep the content of the message secure from interception.

It does not prevent spam, although DMARC can help reduce certain types of spam (such as those that attempt to spoof a domain), it is not designed as a general anti-spam tool. It will not block spam emails that do not attempt to spoof the sender's address.

It does not work without SPF and DKIM, DMARC depends on SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail) to function. Without these two authentication mechanisms configured, DMARC alone cannot operate.

It does not guarantee email deliverability: While DMARC can improve the reputation of a domain by reducing the chance of emails being flagged as fake, it does not guarantee that all legitimate emails will be delivered. Deliverability also depends on other factors such as the reputation of the domain and the configuration of the receiving server.

It does not protect against all types of phishing attacks, DMARC is effective against phishing attacks that involve spoofing a domain in the sender's address, but it does not stop attacks that use visually similar domains or that do not attempt to directly spoof the domain of a known entity.

- **It does not automatically correct SPF and DKIM misconfigurations.** While DMARC can inform the domain administrator about problems with SPF and DKIM settings through its reports, it does not offer automatic solutions to correct these problems. It is the responsibility of the domain administrator to make the necessary adjustments.

- **It does not control the mail handling policy of recipients,** although DMARC allows domain owners to suggest how mails that fail SPF and DKIM checks should be handled, the receiving mail servers have the final say on how to process these mails. This means that different servers may handle DMARC failures in different ways.

- **It does not block the interception of emails,** DMARC cannot prevent an attacker from intercepting or reading emails in transit; its main function is to validate the authenticity of the sender and the integrity of the message.

By understanding what DMARC cannot do, organisations can take additional steps to secure their communications and email systems more effectively.

8.2. Risks of ignorance or non-use of DMARCs

- **Increased spoofing, without DMARC,** attackers can more easily send emails that appear to be from the organisation's domain. This can lead to effective phishing attacks against customers, employees or business partners, who can be tricked into divulging confidential information or performing malicious actions, such as fraudulent money transfers.

- **Damage to domain and brand reputation,** if attackers successfully use a domain to send spam or malware, this can damage the reputation of the associated brand. Customers may lose trust in the organisation, and domains may be blacklisted by email services and spam filters, affecting the delivery of legitimate emails.

- **Loss of control over mailing policy -** by not specifying and enforcing a policy for sending emails through DMARC, organisations lose the opportunity to define and control who can send emails on behalf of their domains, which increases the risk of abuse.
- **Difficult to identify abuses and attacks** without DMARC reporting, organisations may not be aware that their domain is being used for spoofing or other email-related security issues. This delays the ability to respond to incidents and reduces the effectiveness of mitigation measures.
- **Impact on the reliability of communication,** emails sent from domains without a clear DMARC policy may be treated with greater suspicion by receiving mail servers. This can lead to a higher rate of emails being marked as spam or even blocked, affecting effective communication with customers and partners.
- **Vulnerability to targeted attacks,** organisations without DMARC are more vulnerable to spear phishing and other types of targeted attacks, as attackers can exploit the lack of email authentication to conduct more convincing and harder to detect attacks.

Failure to implement DMARC can expose organisations to higher security risks and negative operational and strategic consequences. Therefore, adopting DMARC is an important part of an email security strategy to protect an organisation's resources and integrity.

8.3. Risks of lost e-mail or e-mail being received as spam

When implementing DMARC, it is crucial to **understand the risks associated with the potential loss of legitimate emails.**

DMARC implementation is designed to enhance email security by verifying that messages originating from your domain are authentic and have not been tampered with in transit. Despite its benefits in protecting against impersonation and phishing, the DMARC configuration is not without certain risks, especially related to the potential loss of legitimate emails.

8. Implementation implications

Incorrectly configured SPF and DKIM records, which are essential for DMARC, can lead to increased rejection or quarantining of legitimate mail. This is because emails that do not pass the checks may be automatically rejected or filtered depending on the DMARC policy set (e.g., 'reject' or 'quarantine').

Modifications to the email infrastructure, such as the addition of new sending servers or third-party services that are not included in the SPF records or do not have DKIM configured, may result in authentication failures that affect the delivery of legitimate emails.

Receiving mail servers have the autonomy to decide how to process mails that fail DMARC checks. Even with a policy of 'none', failed mail might be treated more restrictively by some mail providers, which could impact the delivery of legitimate messages, there is a certain dependency on third-party mail handling.

Changes to DNS records, including DMARC, SPF and DKIM, may take time to propagate. During this period, emails may not authenticate correctly, which could temporarily affect the delivery of legitimate emails.

While DMARC can significantly improve the security of your email, it is vital to address these risks through careful planning, accurate configuration and constant monitoring. Hence the recommendation to start a DMARC implementation in monitoring mode (p=none) and gradually adjust the policy as worked out in the document, as the correct configuration and operation of the associated SPF and DKIM records is verified. Special emphasis is also placed on the recommendation to train the technical staff involved on the importance of proper configuration and the need to adapt to changes in the email infrastructure to minimise disruption of legitimate communication.

Currently, some of the large email providers work with large volumes of emails, generating the need to auto-scaling their infrastructures at any time in a timely manner, so it is very important to correctly define DKIM and SPF because with these large providers, due to the volatility and peak load of their needs, there is a risk of not aligning in all cases both parameters, having to work only with the validation of one of them, this is common when using email providers. Due to the needs of these providers, server blocks may be deployed outside the ranges or DKIM keys may not be deployed in time and mails may not be sent correctly aligned. This percentage is residual but should be taken into account.

8.4. Importance of DMARC settings in non-e-mail sending domains

Setting up DMARC on **domains that do not send email is an essential security practice** that is often overlooked, but can have significant implications for protecting a brand's reputation and identity. Even if a domain is not actively sending email, it can still be subject to spoofing and other types of abuse. Implementing DMARC on these domains helps prevent such problems and **does not have the risks discussed above.**

One of the main benefits of setting up DMARC on domains that do not send mail is to **prevent phishing**. Attackers often look for domains that appear legitimate but are not adequately protected with email authentication policies. By configuring DMARC, recommended in this case with a policy of p=reject, you can ensure that no email purportedly sent from that domain is accepted by a receiving server, thus closing off a commonly exploited avenue for phishing attacks.

A brand's reputation can be severely damaged if its domain is used in phishing attacks. This can lead to a loss of customer confidence and possible legal implications, especially in highly regulated industries. Setting up DMARC protects the company name by ensuring that fraudulent emails are not easily accepted by recipients.

By adopting DMARC across all domains under an organisation's control, it **helps to raise the overall standards of email security on the network.** This not only protects individual domains, but also promotes best practices that can foster a more secure online environment.

In some jurisdictions, **regulations exist that require specific protections** for personal information and data security. Configuring DMARC in all domains can be part of complying with these regulations, demonstrating a commitment to information security and the protection of customer data.

Even if a domain does not send mail, if it is spoofed, it could be used to send large amounts of **spam**, which not only affects potential victims but can also result in the domain being blacklisted.

The most important point of this practice is **monitoring and knowledge,** in the event that an attacker or a third party tries to make use of a domain from which it is not planned to send mail, thanks to the reports and the data analysis tools that we have configured (rua and ruf registry) we will obtain **metrics and notifications on the potential fraudulent** use that is detected and we will know at the moment of **the existence of a phishing campaign** that tries to make use of a configured domain.

8.5. Other recommendations

- Ensure **effective collaboration with key email recipients,** including the organisation itself, to facilitate the implementation of DMARC and improve email security management.
- **Develop a plan** with a low level of detail, where you are required to communicate the basics and not go into detail.
- **Identify key email recipients inside and outside the organisation,** including key internal departments and external partners.

For **internal communication,** organise an initial meeting with IT teams and system administrators to communicate the DMARC implementation plan. Explain the importance of the process and how it can impact email reception, focusing on the need to monitor and adjust **spam filters and reception policies to monitor what is received from the organisation itself and how it is treated.**

Establish a regular communication channel (e.g. fortnightly meetings or online chat group) to discuss updates and resolve issues related to DMARC implementation.

For external communication, **send a formal communication to the main external email recipients,** with whom you have a cordial relationship, informing them of the DMARC implementation process. The communication should include the purpose of the implementation, how it might affect mail reception from your domain, and **request their cooperation** in adjusting their receiving systems if necessary.

Establish a process for reviewing and adjusting the DMARC configuration based on internal and external feedback.

Centro Criptológico Nacional

20 ANIVERSARIO

CCN-CERT centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es