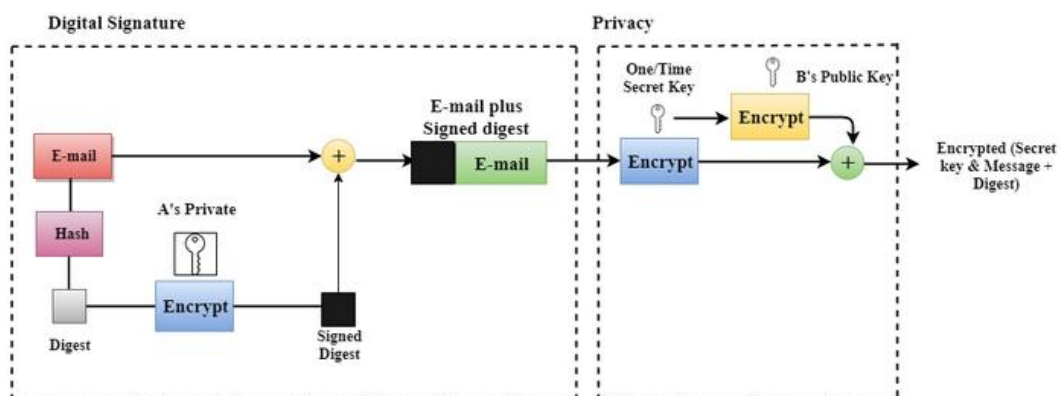


Pretty Good Privacy (PGP)

- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., **privacy, integrity, authentication, and non-repudiation** in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme

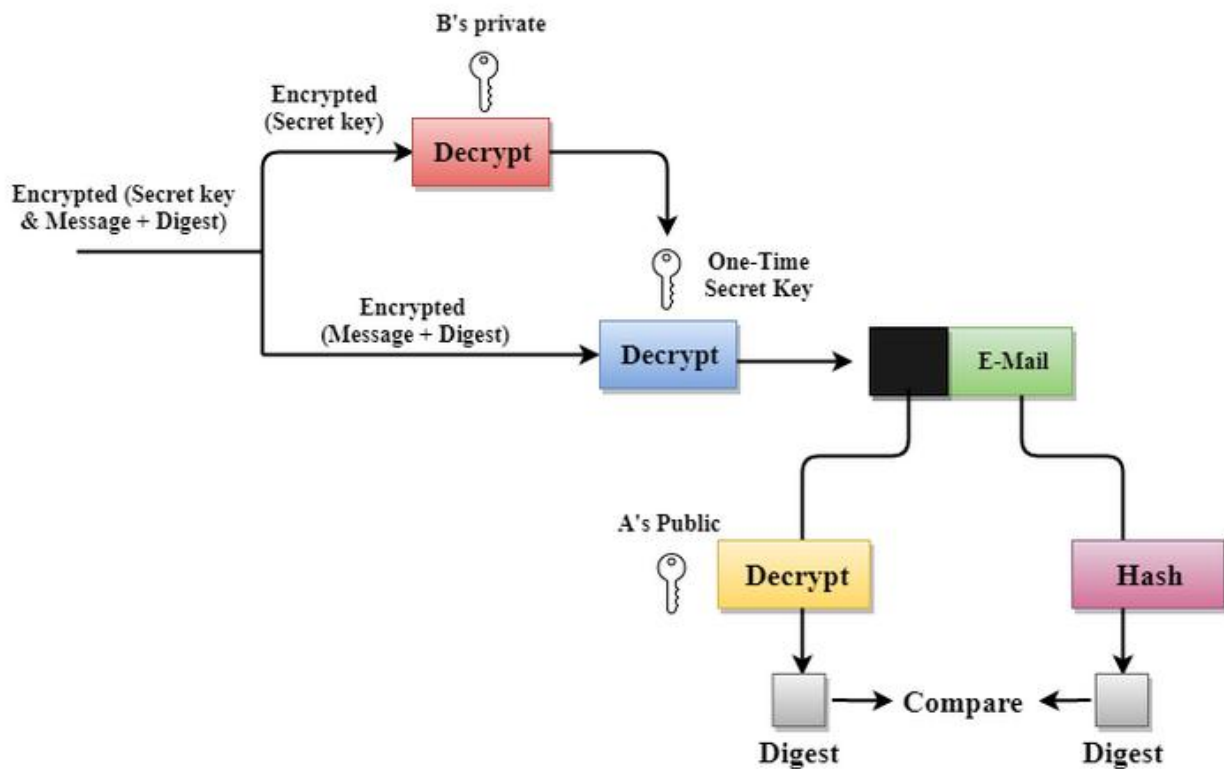
Following are the steps taken by PGP to create secure e-mail at the sender site:

- The e-mail message is hashed by using a hashing function to create a digest.
- The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
- The original message and signed digest are encrypted by using a one-time secret key created by the sender.
- The secret key is encrypted by using a receiver's public key.
- Both the encrypted secret key and the encrypted combination of message and digest are sent together.



Following are the steps taken to show how PGP uses hashing and a combination of three keys to generate the original message:

- The receiver receives the combination of encrypted secret key and message digest is received.
- The encrypted secret key is decrypted by using the receiver's private key to get the one-time secret key.
- The secret key is then used to decrypt the combination of message and digest.
- The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
- Both the digests are compared if both of them are equal means that all the aspects of security are preserved.



Secure/Multipurpose Internet Mail Extensions (S/MIME)

Secure/Multipurpose Internet Mail Extensions (S/MIME) is an end-end encryption protocol for sending digitally signed and encrypted emails that support data confidentiality, authenticity, and integrity.

To understand how S/MIME works we need to understand the following first:

- Digital signatures and signature verification
- Message encryption and decryption
- Public key
- Digital certificates

Digital signatures and verification

With digital signature, S/MIME verifies the identity of the sender of the email. This verification ensures the following:

- Message in the email is the exact message sent by the sender.
- Message is received from the right sender and not someone pretending to be the sender.

Message encryption and decryption

S/MIME uses encryption to protect the content of the email, which ensures that only the receiver can decrypt the content. Encryption creates coded information so that it cannot be read or understood until it is decoded and readable. Message encryption helps with the two key security factors of confidentiality and data integrity.

Public key

S/MIME uses key pairs and asymmetric cryptography. A private key in a key pair belongs only to the sender. If the private key has been used, the owner of that key has used it.

Public key cryptography ensures secure communication between the sender and the receiver. Both have a key-pair, with one being private and the other public.

Public keys are shared between the sender and the receiver. A public key is paired to only one private key. The corresponding public key is used to identify its paired private key and only its paired private key. A public key can be used by multiple recipients.

A key pair can be used to

- Sign and verify a signature
- Encrypt and decrypt the content of an email

S/MIME digital signatures and encryption require each sender and recipient to have it enabled. They also need to send or exchange public keys through digital certificates to identify each other.

Digital certificates

Digital certificates help in delivering the public key in the key pair. A digital certificate is a digital credential that provides information about the identity, validity, and any other required information. Digital certificates are issued by a **certification authority (CA)** and are valid for only a specific period of time.

How does S/MIME work?

S/MIME works based on asymmetric encryption. This means that this protocol uses a **two-key system (Public and Private)** that is mathematically related but different, to encrypt and decrypt an email.

The sender and receiver have their own pair of private and public keys in which the public keys are known to the other party.

A S/MIME certificate needs to be installed on the email clients of both the recipient and the sender to ensure email encryption at both ends. When an email is sent, the sender encrypts the email using the recipient's public key and the recipient decrypts the email using the private key.



Image credits: <https://www.zoho.com/mail/glossary/what-is-s-mime.html>

Benefits of S/MIME

The encryption and digital signing of an email ensure that the data transmitted through email is confidential, and true to its sender. S/MIME protects an email in the following methods:

Email Encryption

The email content is encrypted using the recipient's public key, the moment the sender hits the Send button. Even if the email gets intercepted by anyone, they cannot view the content of the email unless they have access to the private key of the recipient.

Data Confidentiality

The encryption of the email content ensures the confidentiality of the data and attachments sent through the email. Any attempt to view the content of the email is made void as the data can be decrypted only with the help of a private key unique to the recipient.

Digital Signature

The email will be digitally signed along with encryption on installing the S/MIME certificate. The email is signed using the private key of the sender and authenticated by the public key of the recipient. An unaltered digital signature shows that the email content has not been compromised and tampered with.

Signature Authentication

When the sender digitally signs the email using their private key, the recipient validates and authenticates the signature using their public key to ensure that the email is received from a reliable source.

Non-repudiation by the Sender

The digital signature of each sender is unique and is assigned to the user and the domain when the S/MIME certificate is purchased and installed. This voluntarily provides the non-repudiation of the signature by the sender in case of any legal proceedings.

Content Integrity of the Email

When the recipient of a digitally signed email is validated using the public key of the recipient, they're assured of the absence of any alterations in the content of the email and is intact as and when it was sent.

Difference between PGP and S/MIME :

S.NO	PGP	S/MIME
1.	It is designed for processing the plain texts	It is designed to process email as well as many multimedia files.
2.	PGP is less costly as compared to S/MIME.	S/MIME is comparatively expensive.
3.	PGP is good for personal as well as office use.	It is good for industrial use.
4.	PGP is less efficient than S/MIME.	It is more efficient than PGP.
5.	It depends on user key exchange.	It relies on a hierarchically valid certificate for key exchange.
6.	PGP is comparatively less convenient.	It is more convenient than PGP due to the secure transformation of all the applications.
7.	PGP contains 4096 public keys.	It contains only 1024 public keys.
8.	PGP is the standard for strong encryption.	It is also the standard for strong encryption but has some drawbacks.
9.	PGP is also be used in VPNs.	It is not used in VPNs, it is only used in email services.
10.	PGP uses Diffie hellman digital signature .	It uses Elgamal digital signature .
11.	In PGP Trust is established using Web of Trust.	In S/MIME Trust is established using Public Key Infrastructure.
12.	PGP doesn't provides authentication.	S/MIME provides authentication.
13.	PGP is used for Securing text messages only.	S/MIME is used for Securing Messages and attachments.
14.	There is less use of PGP in industry .	S/MIME is widely used in industry.
15.	Convenience of PGP is low.	Convenience of S/MIME is High.
16.	Administrative overhead of PGP is high.	Administrative overhead of S/MIME is low.

Domain Keys Identified Mail (DKIM)

Domain Keys Identified Mail (DKIM) is a digital signature added to every email sent from a given email address.

Why use DKIM?

Imagine the following scenario. You're sending a quick follow-up message to a potential investor after a meeting, *"Yvonne, let me know if you would like to proceed with what we discussed earlier."* Some time goes by, and you never got a reply from Yvonne but you bump into her in another meeting and discreetly mention that email. Puzzled, Yvonne says, *"Mark, I never heard from you back."*

There are many potential reasons for poor deliverability, but, as it turned out, Mark forgot to set up DKIM authentication for his email account. As a result, Yvonne's server wasn't quite sure if it was really Mark emailing her and discarded the message.

The main purpose of DKIM is to prevent spoofing. Email spoofing is changing the original message's content and sending it from an alternative sender that looks like a trusted source. This type of cyber attack is widely used for fraud — for example, someone sending payment request messages from an email address that looks like yours (mark@whatevercompany.io vs. mark@whatever-company.io).

DKIM Header

Here's an example of a DomainKeys Identified Mail record:

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=newyork;  
c=relaxed/simple; q=dns/txt; t=1117574938; x=1118006938;  
h=from:to:subject:date:keywords:keywords;  
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;  
b=dzdVyoFAKcdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ  
VoG4ZHRNiYzR
```

Let's break down the meaning of each element used above:

Tag and its value	Meaning	Mandatory/optional
v=1	Version. Always equals '1'.	Mandatory
a=rsa-sha256	Signing algorithm (the one used to create a DKIM record on the sender's end). Usually, it's either rsa-sha or rsa-sha256. There are other algorithms, but they're not always supported by receiving clients.	Mandatory
d=example.com	The domain of the sender of a message (where DKIM is signed).	Mandatory
s=news	Selector — this includes instructions on which public key to use to resolve a given DKIM (more about this later).	Mandatory
c=relaxed/relaxed	Canonicalization algorithm that's used for both the header and body.	Mandatory
q=dns/txt	Query method that's used to retrieve the public key. By default, it's "dns/txt".	Optional (recommended)
t=1126524832	A timestamp of when the message was signed.	Mandatory
x=1149015927	Expiry time of this DKIM (if an email arrives after the expiry time, the verification will fail even if everything else matches perfectly).	Optional (recommended)
h=from:to:subject:date:keywords:keywords;	List of headers, separated by colons.	Mandatory
bh=MHlzKDU2Nzf3MDEyNzR1Njc5OTAyMjM0MUY3ODlqBLP=	The hashed message body, after being canonicalized with the method from "c" tag and then run through the hash function from "a" tag. (bh – body hash)	Mandatory
b=hyjCnOfAKDdLZdKIc9G1q7LoDWlEniSbzc+yuU2zGrtruF00ldcFVoG4WTHNiYwG	And finally, this is the digital signature of both headers and body, hashed with the very same function.	Mandatory

How does DKIM work?

DKIM signing and receiving happens in three steps:

1. The sender decides what to include in a DKIM record

As a sender, you can limit yourself to only certain parts of header fields (“From”, “To”, “Cc”, “Subject”, etc.), and can also go as far as including the entire header and body in DKIM. You can also choose to add some or all of the optional fields mentioned above.

Technically, the more specific details are included, the more reliable authentication will be. But you need to be careful with this too as even the tiniest details changed by your SMTP email server will lead to a failed DKIM authentication on the receiving side. Think, for example, about “forwarded by...” messages that are added to emails when forwarding them from email clients. If you include your entire body in DKIM, it will now inevitably fail as the body was just modified.

Don’t worry, though. You don’t need to decide on the shape of the DKIM every time you send an email. It’s taken care of automatically by a server that you need to configure just once.

2. The DKIM is created and a message including it is sent

Once the server knows what to include in the DKIM and email sending is initiated, it starts hashing the content. You have already seen how “b” and “bh” tags looked in our example. To give you a further example, here’s how the previous step would look if hashed with the SHA256 method:

```
568291DDA7ECE2594254BC8E7D70DA150968D022021081BB6E3FC40DC9C260D6  
CE328291830AB02CFB1D8CDEC3C2B35C73F92ADF335BCCF38C6784AC9922A8C1
```

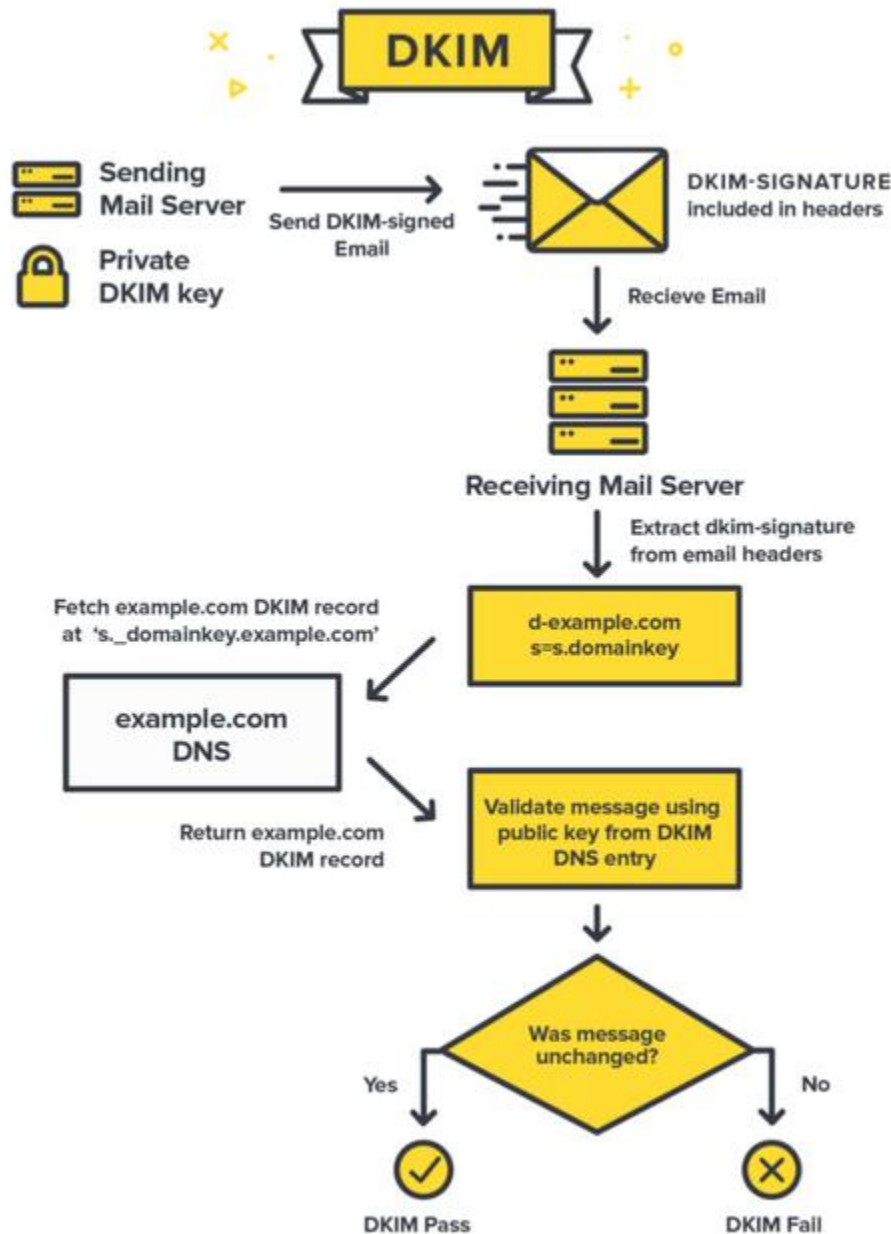
Although it may seem complex, such hashes are extremely easy to decipher with various online tools (try it yourself!). That’s why, before an email is sent, each hash is encrypted with a so-called private key. You can have a separate private key for each selector you use, even if you send all emails from the same domain. This can mean one key for marketing emails, another for transactional emails, and a third for emails sent to vendors. Using different private keys is important for security reasons.

Once everything is set up, the email is sent!

3. A message is received, and the server validates the DKIM signatures

Within seconds, a message is received by the receiving mail server, and it needs to make an important decision — whether to allow the email in or not. When it sees that a DKIM is included with the message, it immediately starts the validation process.

With the domain (“d”) and selector (“s”) fields visible in DKIM, the server can fetch the public key that corresponds to this combination by running an appropriate DNS query (such data is publicly available). Then, with the newly acquired public key and “b” and “h” encrypted fields, the receiving server builds its own hashes and compares them with the ones received in the message. If there’s a match, the authentication is successful. If not, DKIM authorization fails. That doesn’t mean that the message will be discarded, but it lowers its chances of being delivered.



Major misconceptions about DKIM

DKIM encrypts your mail

It doesn't encrypt. DKIM's primary concern is to verify and confirm that the message is intact. The hashes under "bh" and "b" tags offer protection from message modification and replay, including partial protection from identity theft and forgery. A passed DKIM verification test basically means that the email sent has permission to be sent from this domain and that the message content was not altered while in transit.

A DKIM signature can be forged since its details are available in DNS records

No it cannot be forged. DKIM is based on PKI (Public key infrastructure), which means a **pair** of keys is involved. One public and one private. While it is true that the public key is published in the DNS records (and is available for everyone to retrieve), the private key is kept only on the

email service provider server. The private key stays secret and is used to sign messages. The public key cannot sign messages and is used only for verification.

DKIM saves you from spam once and for all

As DKIM digital signature only allows proving that the sender is authorized to send messages from the domain, and the message was not meddled with on the way, **DKIM only lowers the chances of spammers** using forged or stolen email addresses and doesn't **save you from spam once and for all**.

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

DMARC, which stands for “Domain-based Message Authentication, Reporting & Conformance”, is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author (“From:”) domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

Email authentication technologies SPF and DKIM were developed over a decade ago in order to provide greater assurance on the identity of the sender of a message. Adoption of these technologies has steadily increased but the problem of fraudulent and deceptive emails has not abated. It would seem that if senders used these technologies, then email receivers would easily be able to differentiate the fraudulent messages from the ones that properly authenticated to the domain. Unfortunately, it has not worked out that way for a number of reasons.

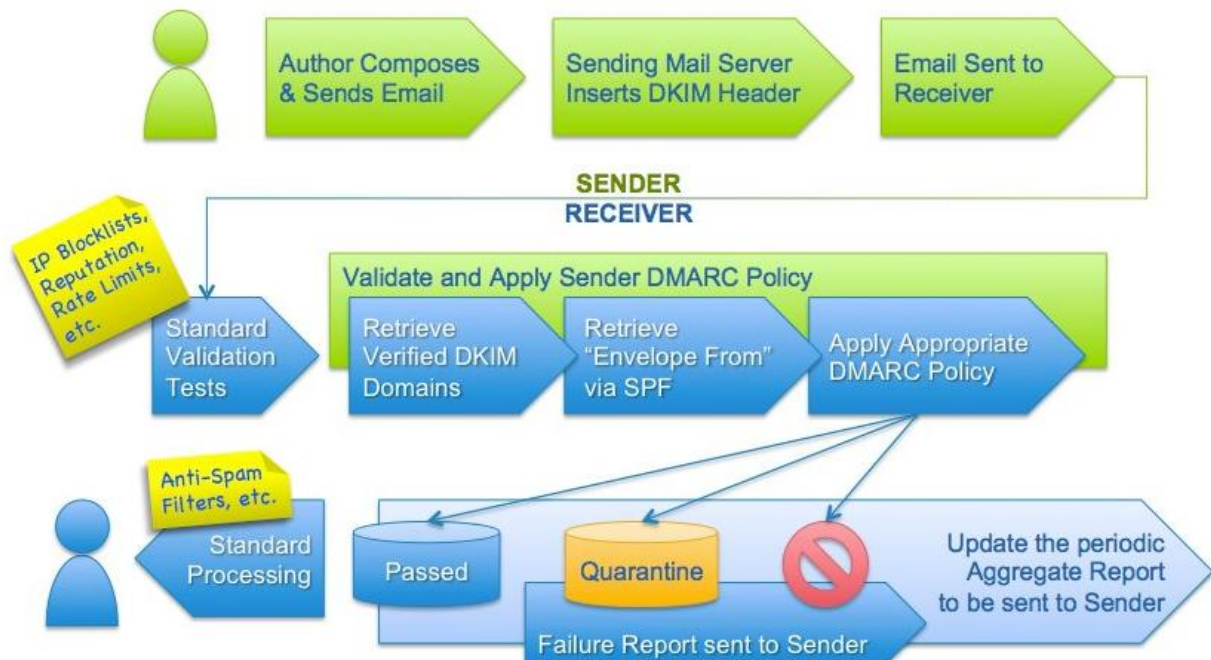
- Many senders have a complex email environment with many systems sending email, often including 3rd party service providers. Ensuring that every message can be authenticated using SPF or DKIM is a complex task, particularly given that these environments are in a perpetual state of flux.
- If a domain owner sends a mix of messages, some of which can be authenticated and others that can't, then email receivers are forced to discern between the legitimate messages that don't authenticate and the fraudulent messages that also don't authenticate. By nature, spam algorithms are error prone and need to constantly evolve to respond to the changing tactics of spammers. The result is that some fraudulent messages will inevitably make their way to the end user's inbox.
- Senders get very poor feedback on their mail authentication deployments. Unless messages bounce back to the sender, there is no way to determine how many legitimate messages are being sent that can't be authenticated or even the scope of the fraudulent emails that are spoofing the sender's domain. This makes troubleshooting mail authentication issues very hard, particularly in complex mail environments.
- Even if a sender has buttoned down their mail authentication infrastructure and all of their legitimate messages can be authenticated, email receivers are wary to reject unauthenticated messages because they cannot be sure that there is not some stream of legitimate messages that are going unsigned.

The only way these problems can be addressed is when senders and receivers share information with each other. Receivers supply senders with information about their mail authentication infrastructure while senders tell receivers what to do when a message is received that does not authenticate.

The goal of DMARC is to build on this system of senders and receivers collaborating to improve mail authentication practices of senders and enable receivers to reject unauthenticated messages.

DMARC and the Email Authentication Process

DMARC is designed to fit into an organization's existing inbound email authentication process. The way it works is to help email receivers determine if the purported message "aligns" with what the receiver knows about the sender. If not, DMARC includes guidance on how to handle the "non-aligned" messages. For example, assuming that a receiver deploys SPF and DKIM, plus its own spam filters, the flow may look something like this:



At a high level, DMARC is designed to satisfy the following requirements:

- Minimize false positives.
- Provide robust authentication reporting.
- Assert sender policy at receivers.
- Reduce successful phishing delivery.
- Work at Internet scale.
- Minimize complexity.

Anatomy of a DMARC resource record in the DNS

DMARC policies are published in the DNS as text (TXT) resource records (RR) and announce what an email receiver should do with non-aligned mail it receives.

Consider an example DMARC TXT RR for the domain “sender.dmarcdomain.com” that reads:

```
"v=DMARC1;p=reject;pct=100;rua=mailto:postmaster@dmarcdomain.com"
```

In this example, the sender requests that the receiver outright reject all non-aligned messages and send a report, in a specified aggregate format, about the rejections to a specified address. If the sender was testing its configuration, it could replace “reject” with “quarantine” which would tell the receiver they shouldn’t necessarily reject the message, but consider quarantining it.

DMARC records follow the extensible “tag-value” syntax for DNS-based key records defined in DKIM. The following chart illustrates some of the available tags:

Tag Name	Purpose	Sample
v	Protocol version	v=DMARC1
pct	Percentage of messages subjected to filtering	pct=20
ruf	Reporting URI for forensic reports	ruf=mailto:authfail@example.com
rua	Reporting URI of aggregate reports	rua=mailto:aggrep@example.com
p	Policy for organizational domain	p=quarantine
sp	Policy for subdomains of the OD	sp=reject
adkim	Alignment mode for DKIM	adkim=s
aspf	Alignment mode for SPF	aspf=r

How does DMARC work?

A DMARC policy allows a sender to indicate that their messages are protected by [SPF](#) and/or [DKIM](#), and tells a receiver what to do if neither of those authentication methods passes – such as junk or reject the message. DMARC removes guesswork from the receiver’s handling of these failed messages, limiting or eliminating the user’s exposure to potentially fraudulent & harmful messages. DMARC also provides a way for the email receiver to report back to the sender about messages that pass and/or fail DMARC evaluation.

Why is DMARC needed?

End users and companies all suffer from the high volume of spam and phishing on the Internet. Over the years several methods have been introduced to try and identify when mail from (for example) IRS.GOV really is, or really isn’t coming from the IRS. However:

- These mechanisms all work in isolation from each other
- Each receiver makes unique decisions about how to evaluate the results
- The legitimate domain owner (e.g. IRS) never gets any feedback

DMARC attempts to address this by providing coordinated, tested methods for:

- Domain owners to:
 - Signal that they are using email authentication (SPF, DKIM)
 - Provide an email address to gather feedback about messages using their domain – legitimate or not
 - A policy to apply to messages that fail authentication (report, quarantine, reject)
- Email receivers to:
 - Be certain a given sending domain is using email authentication
 - Consistently evaluate SPF and DKIM along with what the end user sees in their inbox
 - Determine the domain owner's preference (report, quarantine or reject) for messages that do not pass authentication checks
 - Provide the domain owner with feedback about messages using their domain

Why is DMARC important?

With the rise of the social internet and the ubiquity of e-commerce, spammers and phishers have a tremendous financial incentive to compromise user accounts, enabling theft of passwords, bank accounts, credit cards, and more. Email is easy to spoof and criminals have found spoofing to be a proven way to exploit user trust of well-known brands. Simply inserting the logo of a well known brand into an email gives it instant legitimacy with many users.

Users can't tell a real message from a fake one, and large mailbox providers have to make very difficult (and frequently incorrect) choices about which messages to deliver and which ones might harm users. Senders remain largely unaware of problems with their authentication practices because there's no scalable way for them to indicate they want feedback and where it should be sent. Those attempting new SPF and DKIM deployment proceed very slowly and cautiously because the lack of feedback also means they have no good way to monitor progress and debug problems.

DMARC addresses these issues, helping email senders and receivers work together to better secure emails, protecting users and brands from painfully costly abuse.

Does DMARC block all types of phishing attacks?

No. DMARC is only designed to protect against direct domain spoofing. If the owners/operators of `example.com` use DMARC to protect that domain, it would have no effect on `otherdomain.com` or `example.net` (notice the ".net" vs. ".com").

While impersonating a given domain is a common method used for phishing and other malicious activities, there are other attack vectors that DMARC does not address. For example, DMARC does not address cousin domain attacks (i.e. sending from a domain that looks like the target being abused - e.g. `exampl3.com` vs. `example.com`), or display name abuse (i.e. modifying the "From" field to look as if it comes from the target being abused).

DMARC is designed to protect against direct domain spoofing. When an email is sent by an unauthorized sender (whether it is sent by a malicious actor, or even an unauthorized or non-participating department of the company that owns/operates the domain), DMARC can be used

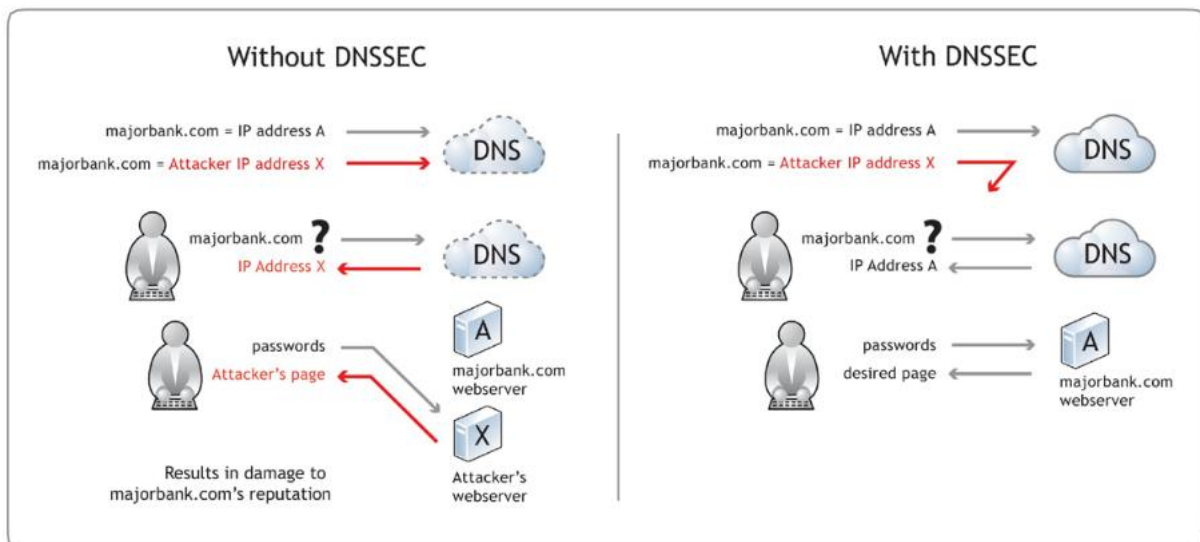
to detect the unauthorized activity and (if so configured) request that those messages be blocked or discarded when they are received.

DNSSEC (DNS Security Extensions)

DNSSEC (short for DNS Security Extensions) adds security to the Domain Name System.

DNSSEC was designed to protect the Internet from certain attacks, such as DNS cache poisoning. It is a set of extensions to DNS, which provide:

- a) origin authentication of DNS data
- b) data integrity
- c) authenticated denial of existence.



Online social networks security and privacy

Positive and negative effects of online social networks based on users perspective

The various positive factors that influence the user to create and use the environments are maintaining social relationship, marketing the product and platforms, rescue efforts and finding common group of people to communicate and share the thoughts.

(1) Maintaining social relationships Social networking sites have proven to be convenient in keeping up with the lives of others who matter to us. It helps to nurture friendship and other social relationships.

(2) Marketing platform Professionals can post work experience and build a network of professionally oriented people on sites such as LinkedIn or Plaxo which are career-building social networks . They help discover better job opportunities. Marketers can influence their audience by posting advertisements on social networking sites.

(3) Rescue efforts Social media sites play a huge role in rescue and recovery efforts during calamities and disasters.

Mobile device security

Mobile phones are becoming ever more popular and are rapidly becoming attractive targets for malicious attacks. Mobile phones face the same security challenges as traditional desktop computers, but their mobility means they are also exposed to a set of risks quite different to those of a computer in a fixed location. Mobile phones can be infected with worms, trojan horses or other virus families, which can compromise your security and privacy or even gain complete control over the device. This guide provides the necessary steps, do's, don'ts & tips to secure your mobile devices.

Mobile Phone Security Threats Categories

- **Mobile Device and Data Security Threats**

Threats related to unauthorised or intentional physical access to mobile phone and Lost or Stolen mobile phones.

Threats related to mobile phone connectivity to unknown systems, phones and networks using technologies like Bluetooth, WiFi, USB etc.

Threats arising from vulnerabilities in Mobile Applications and Operating Systems .

- **Mobile Connectivity Security Threats**
- **Mobile Application and Operating System Security Threats**

Typical impact of attacks against Mobile Phones

- Exposure or Loss of user's personal Information/Data, stored/transmitted through mobile phone.
- Monetary Loss due to malicious software unknowingly utilizing premium and highly priced SMS and Call Services.
- Privacy attacks which includes the tracing of mobile phone location along with private SMSs and calls without user's knowledge.
- Losing control over mobile phone and unknowingly becoming zombie for targeted attacks.

Mitigation against Mobile Device and Data Security Attacks

Do's:

Record IMEI number:

Record the unique 15 digit IMEI number. In case Mobile phone is stolen/lost, this IMEI number is required for registering complaint at Police station and may help in tracking your mobile phone through service provider.

Do's and don'ts for Mobile Device

Enable Device locking:

Use autolock to automatically lock the phone or keypad lock protected by passcode/ security patterns to restrict access to your mobile phone.

Use a PIN to lock SIM card:

Use a PIN (Personal Identification Number) for SIM (Subscriber Identity Module) card to prevent people from making use of it when stolen. After turning on SIM security, each time phone starts it will prompt to enter SIM PIN.

Use password to protect information on the memory card.

Report lost or stolen devices

Report lost or stolen devices immediately to the nearest Police Station and concerned service provider.

Use mobile tracking feature.

Use the feature of Mobile Tracking which could help if the mobile phone is lost/stolen. Every time a new SIM card is inserted in the mobile phone, it would automatically send messages to two preselected phone numbers of your choice, so that you can track your Mobile device

Don'ts:

- Never leave your mobile device unattended.
- Turn off applications [camera, audio/video players] and connections [Bluetooth, infrared, Wi-Fi]

when not in use. Keeping the connections on may pose security issues and also cause to drain out the battery.

Bluetooth is a wireless technology that allows different devices to connect to one another and share data, such as ringtones or photos. Wireless signals transmitted with Bluetooth cover short distances, typically 30 feet (10 meters).

Mitigation against Mobile Connectivity Security Attacks

Do's:

Use Bluetooth in hidden mode so that even if the device is using Bluetooth it is not visible to others.

Change the name of the device to a different name to avoid recognition of your Mobile phone model.

Note: The default name will be the mobile model number for Bluetooth devices.

Put a password while pairing with other devices. The devices with the same password can connect to your computer

Disable Bluetooth when it is not actively transmitting information.

Use Bluetooth with temporary time limit after which it automatically disables so that the device is not available continuously for others.

Back up

Don'ts:

Never allow unknown devices to connect through Bluetooth.

Never switch on Bluetooth continuously.

Never put Bluetooth in always discoverable mode.

Note: Attackers can take advantage of its default always-on, always discoverable settings to launch attacks.

Mitigation against Mobile Application and Operating System Attacks

Application and Mobile Operating System:

- Update the mobile operating system regularly.
- Upgrade the operating system to its latest version.
- Always install applications from trusted sources.
- Consider installing security software from a reputable provider and update them regularly.

- It's always helpful to check the features before downloading an application. Some applications may use your personal data.
- If you're downloading an app from a third party, do a little research to make sure the app is reputable.

Mobile as USB:

The mobile phones can be used as USB memory devices when connected to a computer. A USB cable is provided with the mobile phone to connect to computer. Your mobile's phone memory and memory stick can be accessed as USB devices.

Your mobile's phone memory and memory stick can be accessed as USB devices.

Do's:

When a mobile phone is connected to a personal computer, scan the external phone memory and memory card using an updated anti virus.

Take regular backup of your phone and external memory card because if an event like a system crash or malware penetration occurs, at least your data is safe.

Before transferring the data to Mobile from computer, the data should be scanned with latest Antivirus with all updates.

Don'ts:

Never keep sensitive information like user names/passwords on mobile phones.

Never forward the virus affected data to other Mobiles.

Ten Steps to Smartphone Security

Smartphones continue to grow in popularity and are now as powerful and functional as many computers. It is important to protect your smartphone just like you protect your computer as mobile cybersecurity threats are growing. These mobile security tips can help you reduce the risk of exposure to mobile security threats:

1. Set PINs and passwords. To prevent unauthorized access to your phone, set a password or Personal Identification

Number (PIN) on your phone's home screen as a first line of defense in case your phone is lost or stolen. When possible, use a different password for each of your important log-ins (email, banking, personal sites, etc.). You should configure your phone to automatically lock after five minutes or less when your phone is idle, as well as use the SIM password capability available on most smartphones.

2. Do not modify your smartphone's security settings. Do not alter security settings for convenience. Tampering with your phone's factory settings, jailbreaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone, while making it more susceptible to an attack.

3. Backup and secure your data. You should backup all of the data stored on your phone – such as your contacts, documents, and photos. These files can be stored on your computer, on a removal storage card, or in the cloud. This will allow you to conveniently restore the information to your phone should it be lost, stolen, or otherwise erased.

4. Only install apps from trusted sources. Before downloading an app, conduct research to ensure the app is legitimate. Checking the legitimacy of an app may include such thing as: checking reviews, confirming the legitimacy of the app store, and comparing the app sponsor's official website with the app store link to confirm consistency. Many apps from untrusted sources contain malware that once installed can steal information, install viruses, and cause harm to your phone's contents. There are also apps that warn you if any security risks exist on your phone.

5. Understand app permissions before accepting them. You should be cautious about granting applications access to personal information on your phone or otherwise letting the application have access to perform functions on your phone. Make sure to also check the privacy settings for each app before installing.

6. Install security apps that enable remote location and wiping. An important security feature widely available on smartphones, either by default or as an app, is the ability to remotely locate and erase all of the data stored on your phone,

even if the phone's GPS is off. In the case that you misplace your phone, some applications can activate a loud alarm, even if your phone is on silent. These apps can also help you locate and recover your phone when lost.

7. Accept updates and patches to your smartphone's software. You should keep your phone's operating system software up-to-date by enabling automatic updates or accepting updates when prompted from your service provider, operating system provider, device manufacturer, or application provider. By keeping your operating system current, you reduce the risk of exposure to cyber threats.

8. Be smart on open Wi-Fi networks. When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals. You should limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust or mobile wireless connection to reduce your risk of exposure, especially when accessing personal or sensitive information. Always be aware when clicking web links and be particularly cautious if you are asked to enter account or log-in information.

9. Wipe data on your old phone before you donate, resell, or recycle it. Your smartphone contains personal data you want to keep private when you dispose your old phone. To protect your privacy, completely erase data off of your phone and reset the phone to its initial factory settings. Then, donate, resell, recycle, or otherwise properly dispose of your phone.

10. Report a stolen smartphone. The major wireless service providers, in coordination with the FCC, have established a stolen phone database. If your phone is stolen, you should report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider. This will provide notice to all the major wireless service providers that the

phone has been stolen and will allow for remote “bricking” of the phone so that it cannot be activated on any wireless network without your permission.

.