

یا ذی الامن والامان



امنیت پست الکترونیکی

Network Security Essentials

ویرایش شده توسط: حمید رضا شهریاری

<http://ceit.aut.ac.ir/~shahriari>

فهرست مطالب

- امنیت پست الکترونیکی
- ویژگیهای PGP
- سرویس های PGP
- انواع کلیدهای مورد استفاده
- مدیریت کلید

نیاز به امنیت

- استفاده گسترده از سرویس پست الکترونیکی برای تبادل پیغامها
- نیاز به استفاده از این سرویس برای کاربردهای دیگر
 - به شرط تضمین محرمانگی و احراز هویت
- دو روش برای احراز هویت و ایجاد محرمانگی
 - PGP (Pretty Good Privacy)
 - S/MIME (Secure/Multipurpose Internet Mail Extensions)



قراردادهای پست الکترونیکی

SMTP (Simple Mail Transfer Protocol)



- قرارداد SMTP اصلی ترین و عمومی ترین قرارداد پست الکترونیکی است.
- یک پیغام را همراه با مطالب داخلی و سرآیه آن بصورت کدهای ASCII ارسال می کند.
- SMTP هیچ امنیتی برای داده های ارسال شده فراهم نمی کند.
- داده ها در طول مسیر می توانند خوانده شده یا تغییر داده شوند.
- آدرس فرستنده براحتی قابل تغییر است.

MIME (Multipurpose Internet Mail Extensions)



- MIME یک قرارداد پست الکترونیکی است که برای رفع محدودیت های SMTP و پیغام های متنی پیاده سازی شد.
- MIME هیچ گونه امنیتی فراهم نمی کند.

معرفی PGP

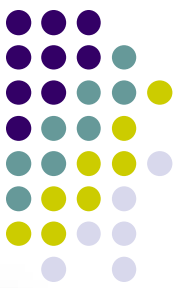


- ارائه شده توسط آقای Philip R. Zimmermann در سال ۱۹۹۱
- باعث ایجاد پرونده قضایی علیه وی تا سه سال شد!



ویژگیهای PGP

- استفاده گسترده از آن به عنوان سرویس پست الکترونیکی امن
- استفاده از بهترین الگوریتمهای رمزنگاری موجود و ترکیب آنها در یک برنامه کاربردی چند منظوره
- قابلیت اجرای مستقل از ماشین و پردازنده (Unix، PC، Macintosh...)
- عدم انحصار توسط دولت یا شرکت خاص
- دسترسی به متن باز و بسته نرم افزاری آن مجانی است.
- در حال استاندارد شدن
- (RFC 3156; MIME Security with OpenPGP)



PGP basic Services

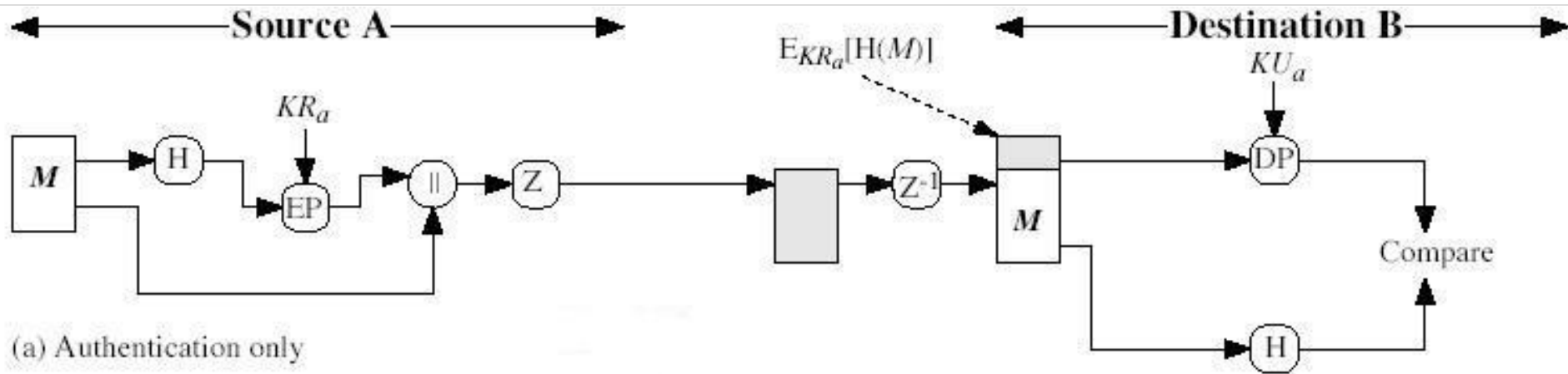
Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

PGP سرویسهای

احراز اصالت

- تولید چکیده ۱۶۰ بیتی از پیغام اولیه با استفاده از SHA-1
- استفاده از RSA و کلید خصوصی فرستنده برای رمز کردن چکیده
- الحاق چکیده رمز شده به انتهای پیغام
- استفاده از RSA با کلید عمومی فرستنده برای بازیابی چکیده در سمت گیرنده
- تولید چکیده پیغام جدید توسط گیرنده و مقایسه آن با چکیده بازیابی شده

PGP- Authentication Only

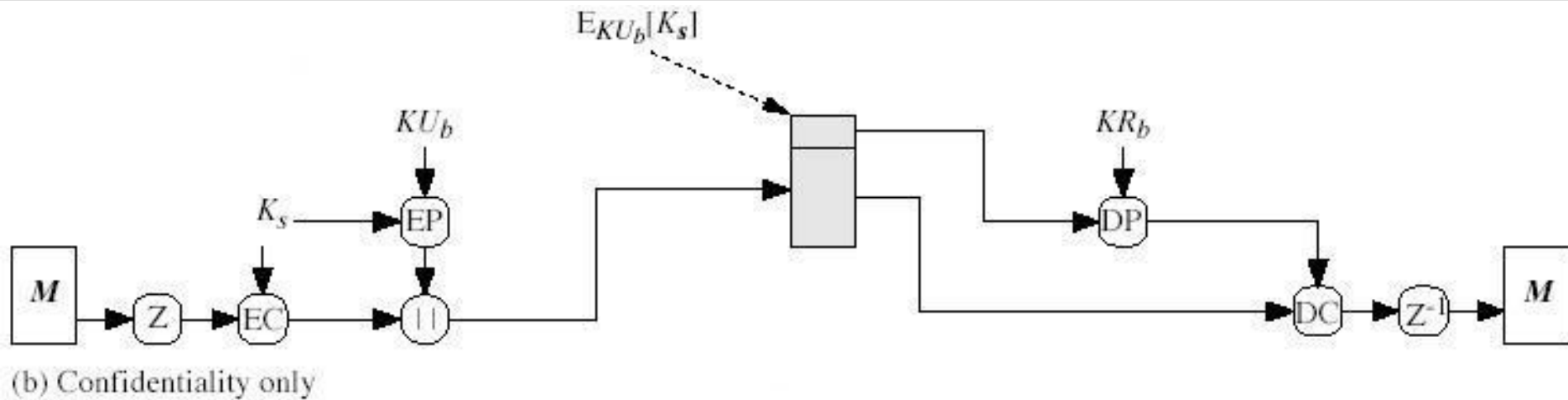


PGP سرویسهای

محرمانگی

- ☐ استفاده از عدد تصادفی ۱۲۸ بیتی بعنوان کلید جلسه ویژه پیغام جاری
- ☐ رمزکردن پیغام با استفاده از CAST-128 یا IDEA یا 3DES و کلید جلسه تولید شده
- ☐ رمزکردن کلید جلسه با استفاده از الگوریتم RSA و کلید عمومی گیرنده
- ☐ الحاق کلید رمز شده به پیغام و ارسال آن
- ☐ استفاده از RSA با کلید خصوصی گیرنده برای رمزگشایی و بازیابی کلید جلسه
- ☐ رمزگشایی پیغام دریافت شده با استفاده از کلید جلسه

PGP- Confidentiality Only



PGP سرویسهای

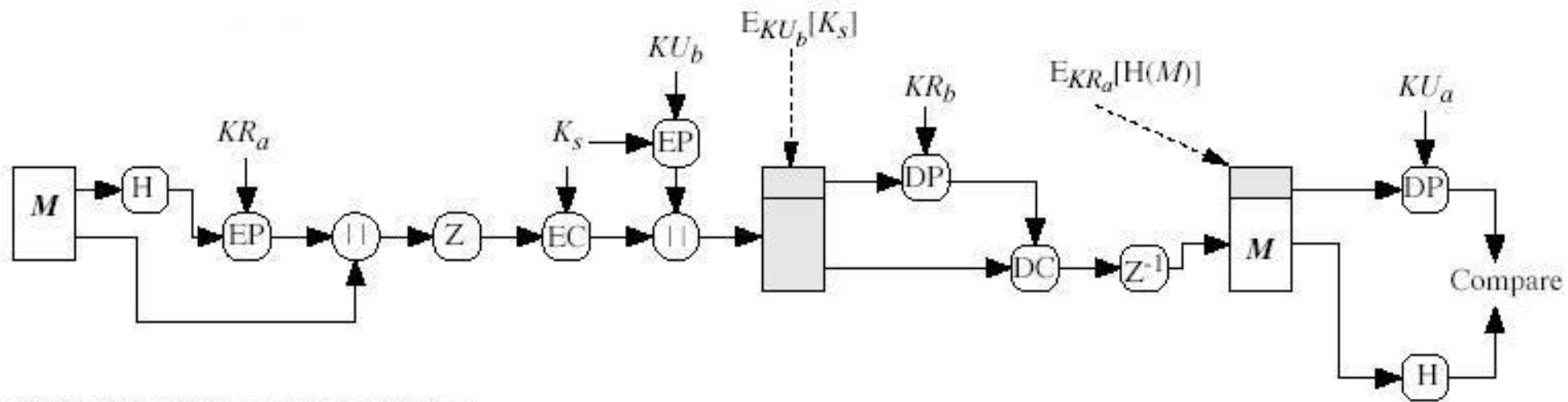
□ محرمانگی + احراز هویت

- تولید امضاء و الحاق آن به متن
- رمز کردن مجموعه امضا و متن با استفاده از CAST-128
- الحاق کلید جلسه رمز شده با الگوریتم RSA به مجموعه فوق

□ چرا اول امضاء رقمی انجام می شود و سپس رمز گذاری؟

- با این روش شخص ثالث برای تایید امضاء هیچ نوع نگرانی در رابطه با کلید جلسه نخواهد داشت.

Confidentiality & Authentication



(c) Confidentiality and authentication

PGP سرویسهای

فشرده سازی

- به صورت پیش فرض فشرده سازی پس از امضاء و قبل از رمزگذاری انجام می شود.
- چرا پس از امضاء؟
 - باید بتوان پیام و امضاء را برای تایید بعدی و بدون نیاز به فشرده سازی و یا بازگشایی مجدد ذخیره نمود.
 - در صورتی که طرفین از مکانیسم های فشرده سازی متفاوت استفاده می کنند، در تایید امضا تداخلی ایجاد نشود.
- چرا قبل از رمزگذاری؟
 - کاهش حجم و افزونگی متنی که باید رمز شود
 - کاهش اطلاعات آماری پیغام

PGP سرویسهای

حفظ سازگاری

❑ مشکل:

■ فرستادن داده های باینری از طریق سرویس های پست الکترونیکی که تنها برای ارسال متن ASCII طراحی شده اند.

❑ راه حل:

■ تبدیل داده های خام باینری به متن ASCII :

❑ استفاده از الگوریتم Radix-64

■ تبدیل ۳ بایت به ۴ کاراکتر قابل چاپ ASCII

■ اضافه کردن CRC به انتهای آن

■ توسعه متن به اندازه ۳۳٪ به دلیل استفاده از Radix-64 و فشرده سازی به اندازه ۵۰٪-

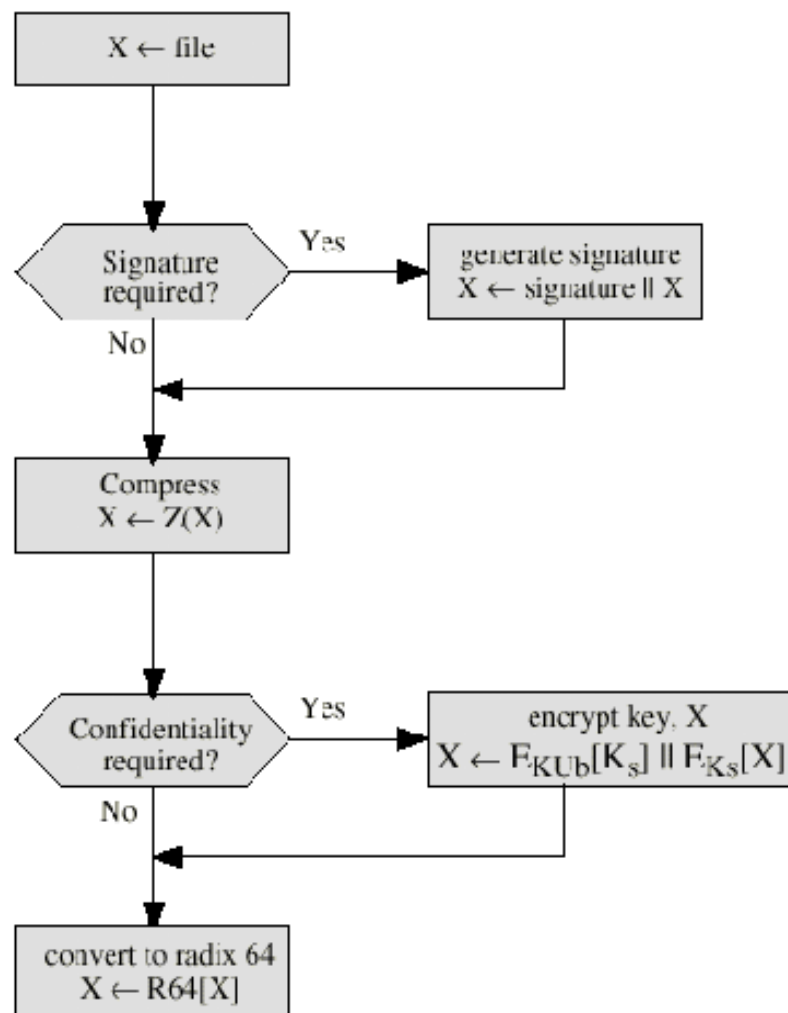
$$1.33 \times 0.5 = 0.665 < --$$

■ نتیجه : فشرده سازی به اندازه 1/3

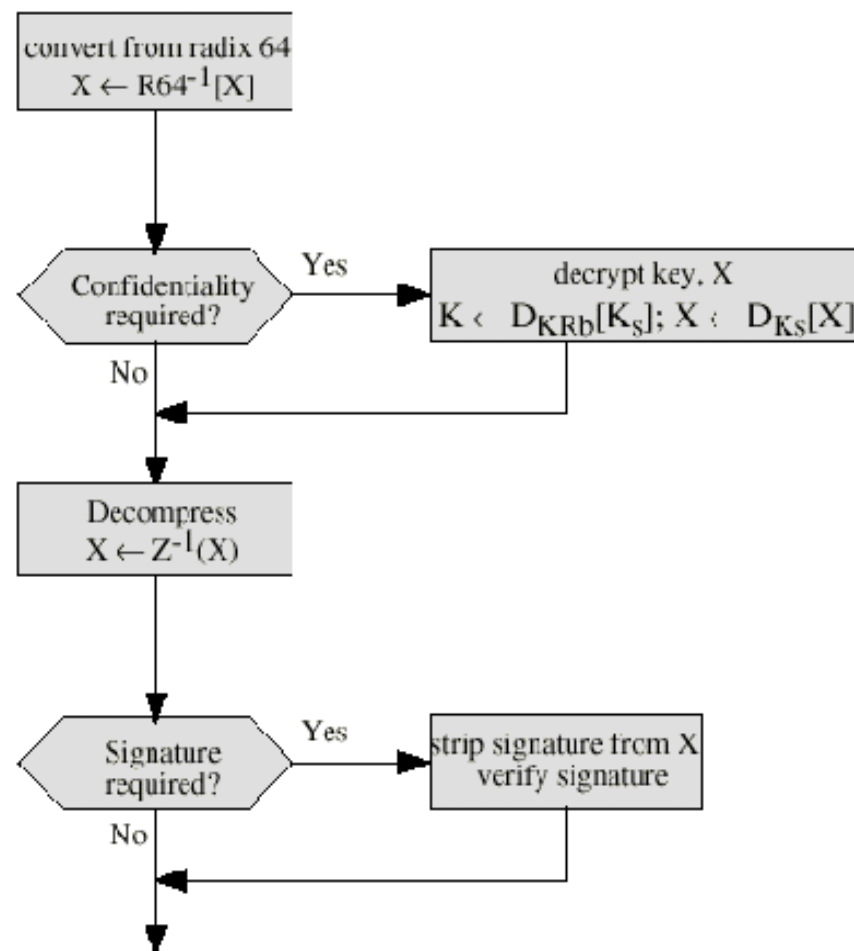
PGP سرویسهای

قطعه بندی

- محدودیت سرویس دهنده های ایمیل در اندازه پیغام ارسالی
- انجام قطعه بندی توسط PGP به صورت خودکار و پس از انجام کلیه محاسبات و تبدیلات
- ارسال کلید جلسه و تایید امضاء رقمی فقط در ابتدای قطعه اول
- بازیابی پیغام اصلی از روی قطعه ها در سمت گیرنده (قبل از انجام هر پردازشی)



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

Figure 5.2 Transmission and Reception of PGP Messages

کلیدهای مورد استفاده

PGP از چهار نوع کلید بهره می برد:

- کلید متقارن یکبار مصرف (کلید جلسه)
- کلید عمومی
- کلید خصوصی
- کلید متقارن حاصل از گذرواژه (برای رمز کردن کلیدهای خصوصی)

کلیدهای مورد استفاده

کلید جلسه

- به صورت تصادفی و یکبار مصرف ایجاد می گردد
- الگوریتم تولید عدد تصادفی خود CAST-128 می باشد طبق استاندارد ANSI X12.17
- الگوریتم از روی کلیدهای فشرده شده روی صفحه کلید مقدار اولیه می گیرد.
- سپس کلیدهای جلسه را به صورت CFB تولید می کند

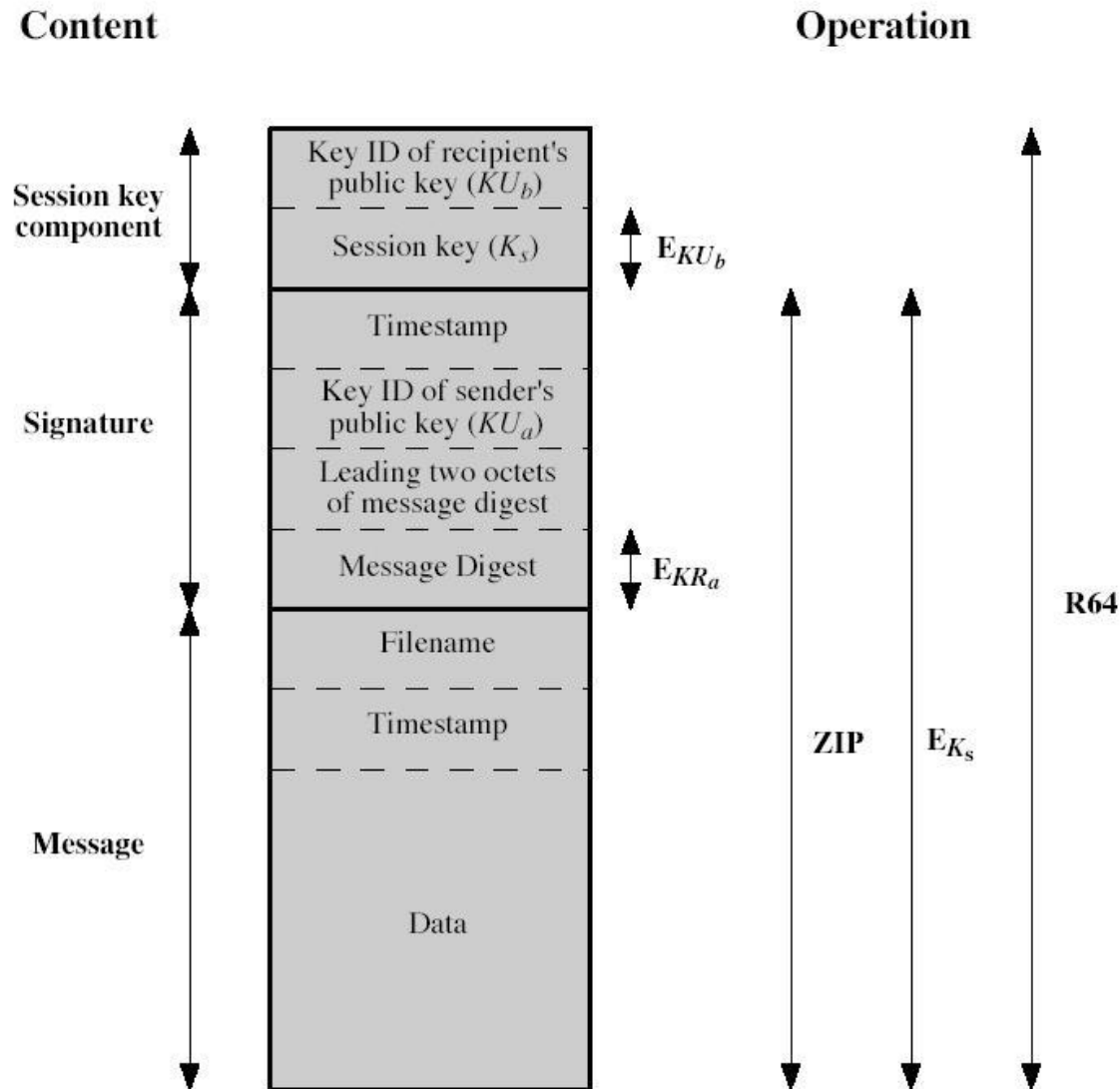
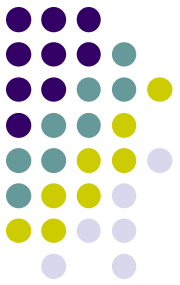
کلیدهای مورد استفاده

مسئله : امکان داشتن چند زوج کلید نامتقارن برای ارتباط با گروههای مختلف.

راه حل : مشخص نمودن کلید استفاده شده بوسیله یک شناسه (Key Identifier)

- استفاده از مقدار $(KU_a \bmod 2^{64})$ به عنوان شناسه
- احتمال برخورد بسیار پایین است.

Format of PGP Message



کلیدهای مورد استفاده

دسته کلید خصوصی (Private Key Ring)

برای مدیریت کلیدهای نا متقارن استفاده می شود. شامل موارد زیر است:

- ۱ - زمان تولید کلید
- ۲ - شناسه کلید
- ۳ - کلید عمومی
- ۴ - کلید خصوصی (بصورت رمز شده)
- ۵ - شناسه مالک کلید

□ کلید خصوصی توسط کلید متقارنی که بصورت چکیده ای از گذرواژه کاربر می باشد، رمز می شود

□ جدول کلیدهای خصوصی روی ماشین صاحبش ذخیره می شود.

جدول کلید خصوصی

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
⋮	⋮	⋮	⋮	⋮
T_i	$KU_i \bmod 2^{64}$	KU_i	$E_{H(P_i)}[KR_i]$	User i
⋮	⋮	⋮	⋮	⋮

کلیدهای مورد استفاده

دسته کلید عمومی (Public Key Ring)

شامل موارد زیر است:

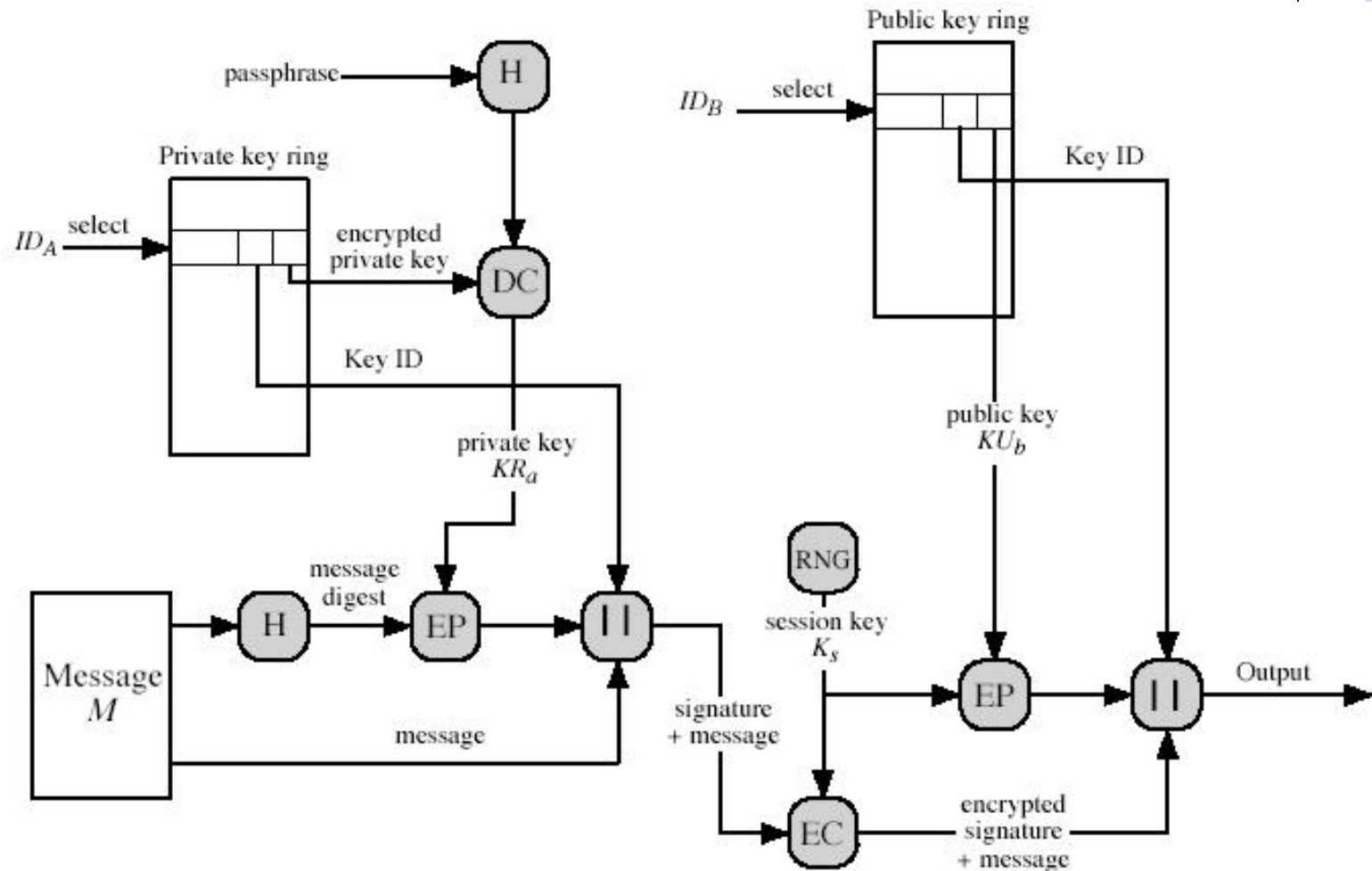
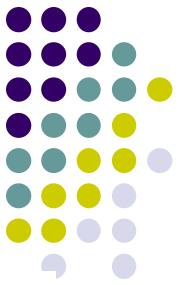
- ۱- زمان تولید کلید
- ۲- شناسه کلید
- ۳- کلید عمومی
- ۴- شناسه کاربر
- ۵- و چند فیلد دیگر جهت امنیت بیشتر

این جدول شامل همه کلیدهای عمومی کاربران دیگر که برای این کاربر مشخص است، می باشد.

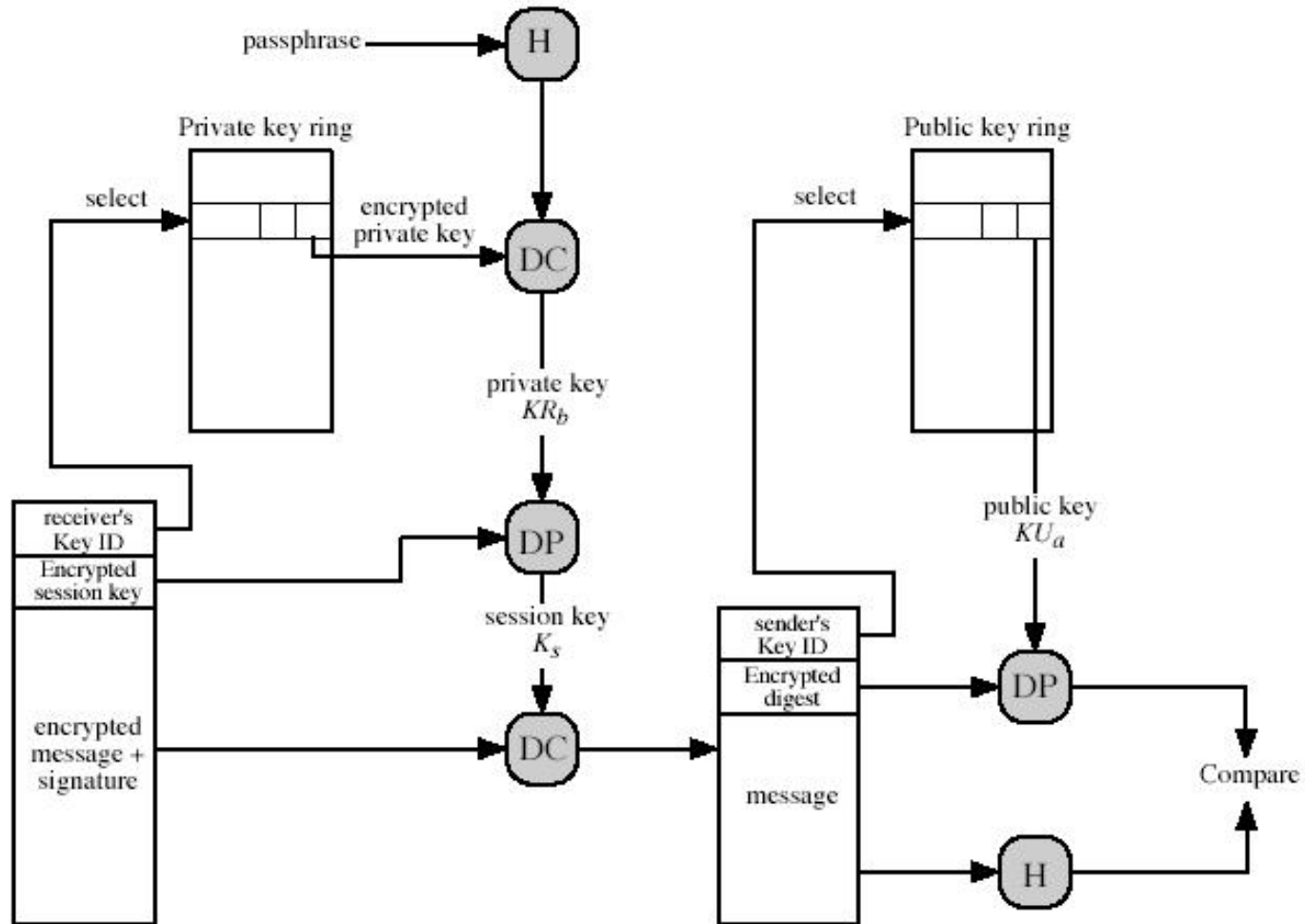
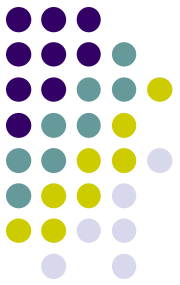
Public Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
T_i	$KU_i \bmod 2^{64}$	Ku_i	trust_flag _i	User i	trust_flag _i		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

PGP Message Generation



PGP Reception



مدیریت کلید

مشکل: در جدول کلیدهای عمومی A ، یک کلید به نظر می رسد متعلق به کاربر B است، ولی در واقع متعلق به C است. در نتیجه C می تواند:

- بجای B به A پیغام بفرستد
- پیغامهای ارسال شده از A به سمت B را بخواند

مدیریت کلید عمومی در PGP

□ ارسال کلید عمومی با خاصیت احراز اصالت

■ انتقال بصورت فیزیکی

□ در شبکه این کار غیر عملی است.

■ انتقال بصورت الکترونیکی و تایید توسط تلفن یا...

□ چکیده‌ای از کلید دریافتی از طریق تلفن با مالک بررسی شود.

■ انتقال توسط فرد مطمئنی که کلید عمومی وی در اختیار است.

□ کلید عمومی کاربر B توسط کاربر شناخته شده D امضاء و به کاربر A ارسال می‌شود.

■ انتقال بصورت گواهی تایید شده توسط مرجع قابل اعتماد.

مدیریت کلید

□ PGP برای مدیریت کلیدهای عمومی بجای CA از مدلی بنام اعتماد (Trust) استفاده می کند.

□ فیلدهای Trust

۱. فیلد Key Legitimacy: بیانگر میزان اعتماد PGP به اعتبار کلید عمومی.

۲. فیلد Signature trust: هر مدخل که یک کلید عمومی کاربری را مشخص می کند دارای چند امضا است. هر یک از این امضاها دارای یک درجه اعتماد هستند.

□ فیلد Key legitimacy از روی همین فیلدهای Sig. Trust محاسبه می شود.

۳. فیلد Owner trust: بیانگر میزان اعتماد به صاحب کلید برای تایید اعتبار کلیدهای عمومی دیگر (گواهی).

- هر سه فیلد فوق در داخل یک بایت تحت عنوان trust flag نگهداری می شوند.

مدیریت کلید

- هنگامی که A یک کلید عمومی جدید در دسته کلید درج می کند،
 - اگر کلید متعلق به A باشد: Ultimate trust
 - در غیراین صورت A باید شخصا مقداری وارد کند:
- Unkown, untrusted, marginally trusted, completely trusted
- هنگامی که امضایی برای کلید عمومی اضافه می شود:
 - اگر امضا کننده در دسته کلید، دارای کلید عمومی باشد، فیلد owner trust این کلید عمومی به فیلد sig. Trust امضا کپی می شود، در غیر این صورت unknown user
- فیلد legitimacy trust بر اساس فیلدهای sig. Trust محاسبه می شود.
 - اگر حداقل یک فیلد دارای مقدار ultimate باشند: complete
 - در غیر این صورت بر اساس وزن امضاها محاسبه میشود.

Trust Flag Bytes

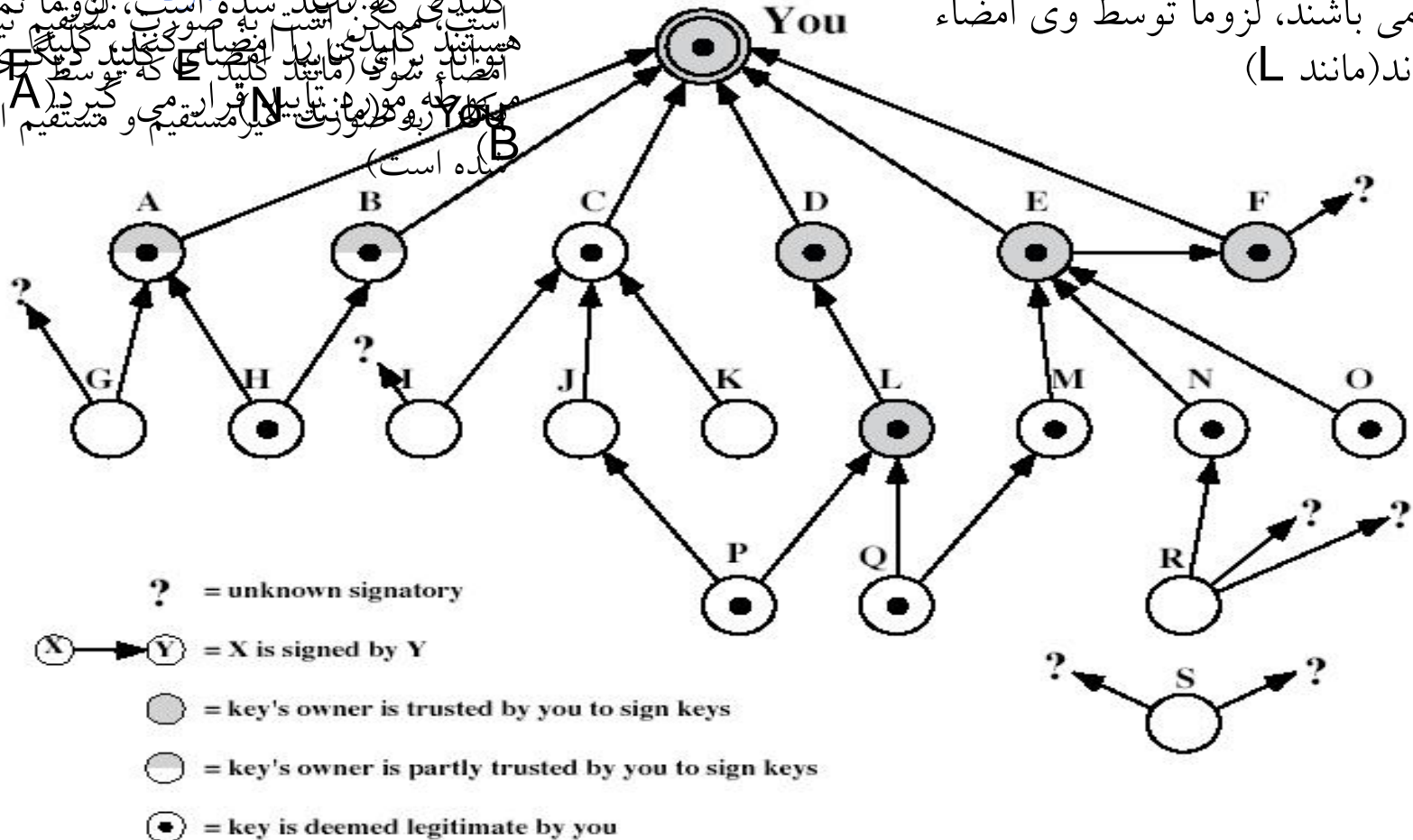
(a) Trust Assigned to Public-Key Owner (appears after key packet; user defined)	(b) Trust Assigned to Public Key/User ID Pair (appears after User ID packet; computed by PGP)	(c) Trust Assigned to Signature (appears after signature packet; cached copy of OWNERTRUST for this signator)
<p>OWNERTRUST Field</p> <ul style="list-style-type: none"> — undefined trust — unknown user — usually not trusted to sign other keys — usually trusted to sign other keys — always trusted to sign other keys — this key is present in secret key ring (ultimate trust) <p>BUCKSTOP bit</p> <ul style="list-style-type: none"> — set if this key appears in secret key ring 	<p>KEYLEGIT Field</p> <ul style="list-style-type: none"> — unknown or undefined trust — key ownership not trusted — marginal trust in key ownership — complete trust in key ownership <p>WARNONLY bit</p> <ul style="list-style-type: none"> — set if user wants only to be warned when key that is not fully validated is used for encryption 	<p>SIGTRUST Field</p> <ul style="list-style-type: none"> — undefined trust — unknown user — usually not trusted to sign other keys — usually trusted to sign other keys — always trusted to sign other keys — this key is present in secret key ring (ultimate trust) <p>CONTIG bit</p> <ul style="list-style-type: none"> — set if signature leads up a contiguous trusted certification path back to the ultimately trusted key ring owner



Trust Model Example

کلید کاربری که بطور غیر مستقیم امضاء شده
 است و کلید دیگری که بر آن امضاء شده است، این و ما نمی
 هستیم که کلید را با امضاء کننده کلید
 امضاء برای (ما) امضاء کنیم که توسط (A) و
 می که (A) و (B) امضاء کرده اند (ما) امضاء
 (B) (ما) امضاء کرده است

کلیدهای کار برانی که مورد اعتماد یک
 کاربر می باشند، لزوماً توسط وی امضاء
 نشده اند (مانند L)



مدیریت کلید

چند نکته در مورد شکل قبل

۱. کلیدهای کار برانی که مورد اعتماد یک کاربر می باشند، لزوماً توسط وی امضاء نشده اند (مانند L)
۲. اگر دو کاربری که معمولاً قابل اعتماد هستند کلیدی را امضاء کنند، کلید مربوطه مورد تایید قرار می گیرد (A و B)
۳. کلیدی که تایید شده است، لزوماً نمی تواند برای تایید امضای کلید دیگری بکار رود (مانند N)
۴. کلید کاربری که بطور غیرمستقیم امضاء شده است، ممکن است به صورت مستقیم نیز امضاء شود (مانند کلید E که توسط F و You به صورت غیرمستقیم و مستقیم امضا شده است)

Email Security

S/MIME

Simple Mail Transfer Protocol (SMTP, RFC 822)

- محدودیتهای SMTP : عدم توانایی یا مشکل در انتقال
 - فایل‌های باینری یا اجرایی (مانند jpeg)
 - کاراکترهای غیر لاتین (غیر اسکی)
 - پیام بزرگتر از یک اندازه خاص
 - مشکلات تبدیل در ASCII و EBCDIC
 - خطوط بزرگتر از حد خاص

فیلدهای سرآیند در MIME

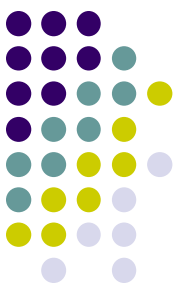
MIME-Version ☐

Content-Type ☐

Content-Transfer-Encoding ☐ نحوه کدگذاری مثلا
RADIX64

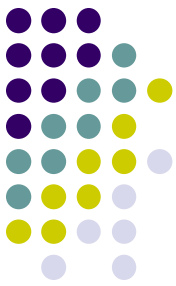
Content-ID ☐ رشته منحصر به فرد

Content Description ☐ هنگامی که متن قابل خواندن
نیست (مثلا mpeg)



MIME Content Types

Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript format.
	octet-stream	General binary data consisting of 8-bit bytes.



```
MIME-Version: 1.0
From: Nathaniel Borenstein <nbs@bellcore.com>
To: Ned Freed <ned@innosoft.com>
Subject: A multipart example
Content-Type: multipart/mixed;
    boundary=unique-boundary-1
This is the preamble area of a multipart message. Mail readers that understand multipart format should ignore this preamble.
If you are reading this text, you might want to consider changing to a mail reader that understands how to properly display
multipart messages.

--unique-boundary-1
...Some text appears here...
[Note that the preceding blank line means no header fields were given and this is text, with charset US ASCII. It could have
been done with explicit typing as in the next part.]

--unique-boundary-1
Content-type: text/plain; charset=US-ASCII
This could have been part of the previous part, but illustrates explicit versus implicit typing of body parts.

--unique-boundary-1
Content-Type: multipart/parallel; boundary=unique-boundary-2

--unique-boundary-2
Content-Type: audio/basic
Content-Transfer-Encoding: base64
... base64-encoded 8000 Hz single-channel mu-law-format audio data goes here....

--unique-boundary-2
Content-Type: image/jpeg
Content-Transfer-Encoding: base64
... base64-encoded image data goes here....

--unique-boundary-2--
--unique-boundary-1
Content-type: text/enriched

This is <bold><italic>richtext.</italic></bold> <smaller>as defined in RFC 1896</smaller>

Isn't it <bigger><bigger>cool?</bigger></bigger>

--unique-boundary-1
Content-Type: message/rfc822

From: (mailbox in US-ASCII)
To: (address in US-ASCII)
Subject: (subject in US-ASCII)
Content-Type: Text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: Quoted-printable

... Additional text in ISO-8859-1 goes here ...

--unique-boundary-1--
```

Figure 8.3 Example MIME Message Structure

S/MIME Functions

□ **Enveloped Data**: رمزگذاری داده و کلید جلسه برای گیرنده

□ **Signed Data**: چکیده پیام با کلید خصوصی فرستنده رمز می شود.

□ **Clear-Signed Data**: فقط امضا می شود.

□ **Signed and Enveloped Data**: هم امضا و هم رمز می شود

S/MIME Functionality

Enveloped data

- Consists of encrypted content of any type and encrypted content encryption keys for one or more recipients

Signed data

- A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer
- The content plus signature are then encoded using base64 encoding
- A signed data message can only be viewed by a recipient with S/MIME capability

S/MIME

Clear-signed data

- Only the digital signature is encoded using base64
- As a result recipients without S/MIME capability can view the message content, although they cannot verify the signature

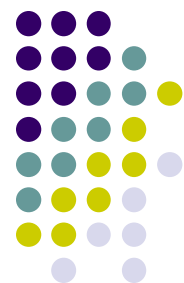
Signed and enveloped data

- Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted

الگوریتمهای مورد استفاده

- ❑ **Message Digesting:** SHA-1 and MD5
- ❑ **Digital Signatures:** DSS
- ❑ **Secret-Key Encryption:** Triple-DES, RC2/40 (exportable)
- ❑ **Public-Private Key Encryption:** RSA with key sizes of 512 and 1024 bits, and Diffie-Hellman (for session keys).

Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-1. Receiver SHOULD support MD5 for backward compatibility.
Encrypt message digest to form a digital signature.	Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption. Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
Encrypt session key for transmission with a message.	Sending and receiving agents SHOULD support Diffie-Hellman. Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits.
Encrypt message for transmission with a one-time session key.	Sending and receiving agents MUST support encryption with tripleDES Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.
Create a message authentication code	Receiving agents MUST support HMAC with SHA-1. Sending agents SHOULD support HMAC with SHA-1.



Cryptographic

Algorithms

Used in

S/MIME

S/MIME Content Types

Type	Subtype	smime Parameter	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs7-mime	signedData	A signed S/MIME entity.
	pkcs7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs7-mime	degenerate signedData	An entity containing only public-key certificates.
	pkcs7-mime	Compressed Data	A compressed S/MIME entity.
	pkcs7-signature	signedData	The content type of the signature subpart of a multipart/signed message.

S/MIME

□ S/MIME از گواهی های کلید عمومی X.509 نسخه ۳ که توسط یک CA امضا شده باشد استفاده می کند.

□ وظایف:

■ تولید کلید : Diffie-Hellman, DSS, RSA

■ ثبت کلید (Registration): کلیدهای عمومی باید توسط مرکز گواهی ثبت شوند.

■ ذخیره گواهی ها: گواهی ها به صورت محلی ذخیره می شوند

■ رمز گذاری و امضای داده

S/MIME

مثال: ☐

Verisign (www.verisign.com) ☐

Class-1 ☐ آدرس email فرستنده با فرستادن یک سری اطلاعات تایید می شود.

Class-2 ☐ آدرس پستی هم بررسی و تایید می شود.

Class-3 ☐ خریدار باید حضورا مراجعه کند یا مدارک رسمی بفرستد.

DomainKeys Identified Mail (DKIM)

- ❑ A specification for cryptographically signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream
 - ❑ Message recipients can verify the signature by querying the signer's domain directly to retrieve the appropriate public key and can thereby confirm that the message was attested to by a party in possession of the private key for the signing domain
 - ❑ Proposed Internet Standard RFC 4871
 - ❑ Has been widely adopted by a range of e-mail providers and Internet Service Providers (ISPs)
-

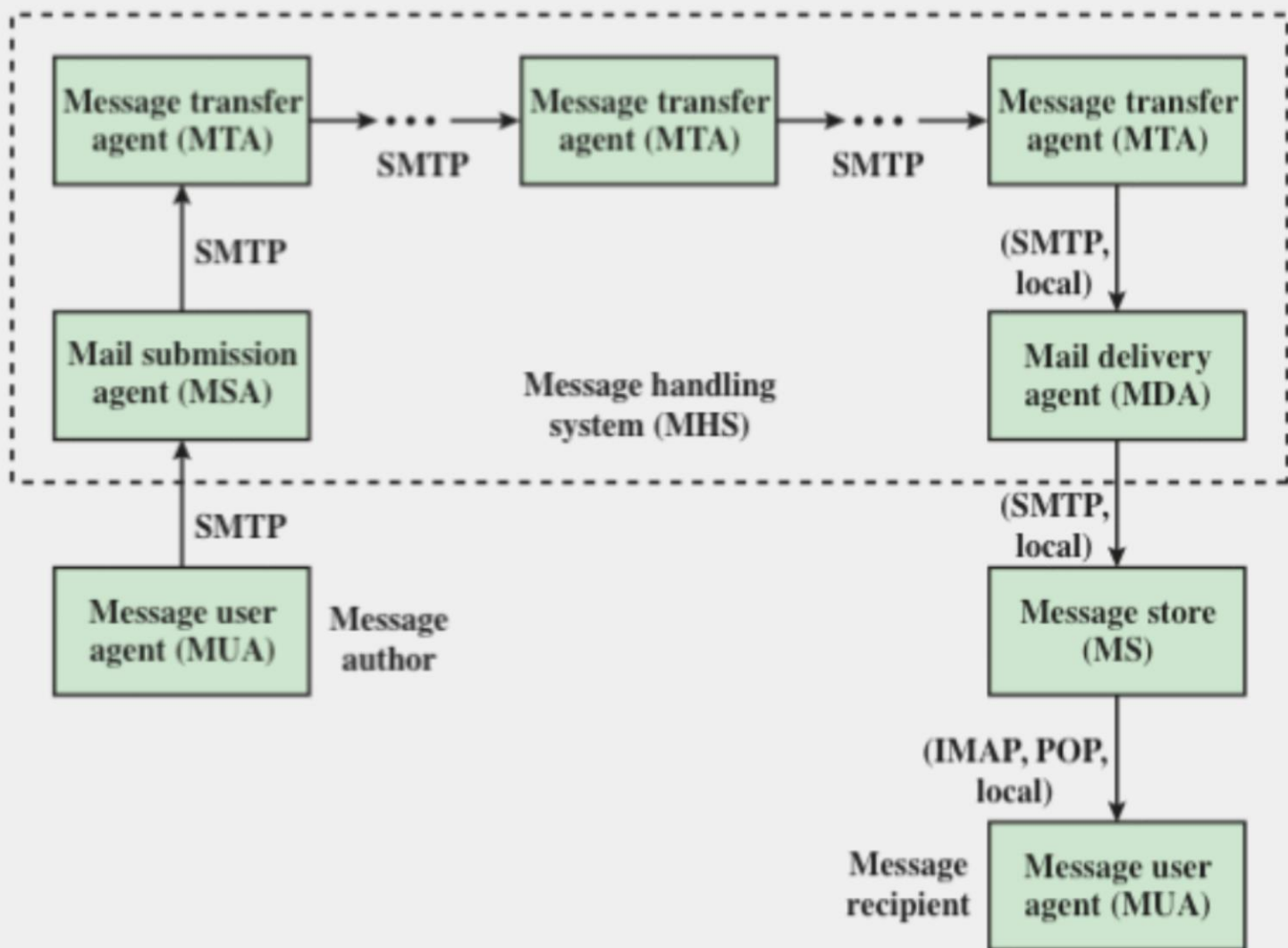


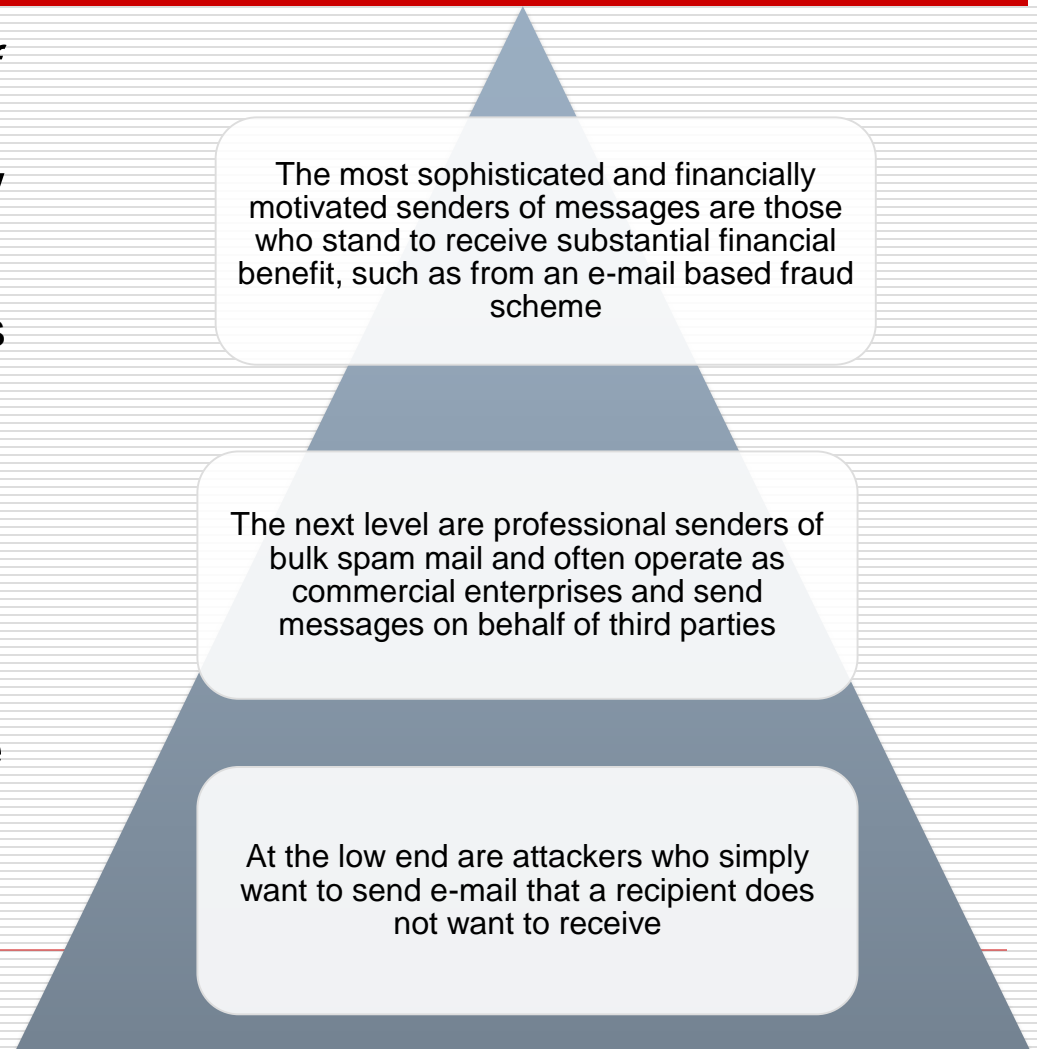
Figure 8.4 Function Modules and Standardized Protocols Used Between Them

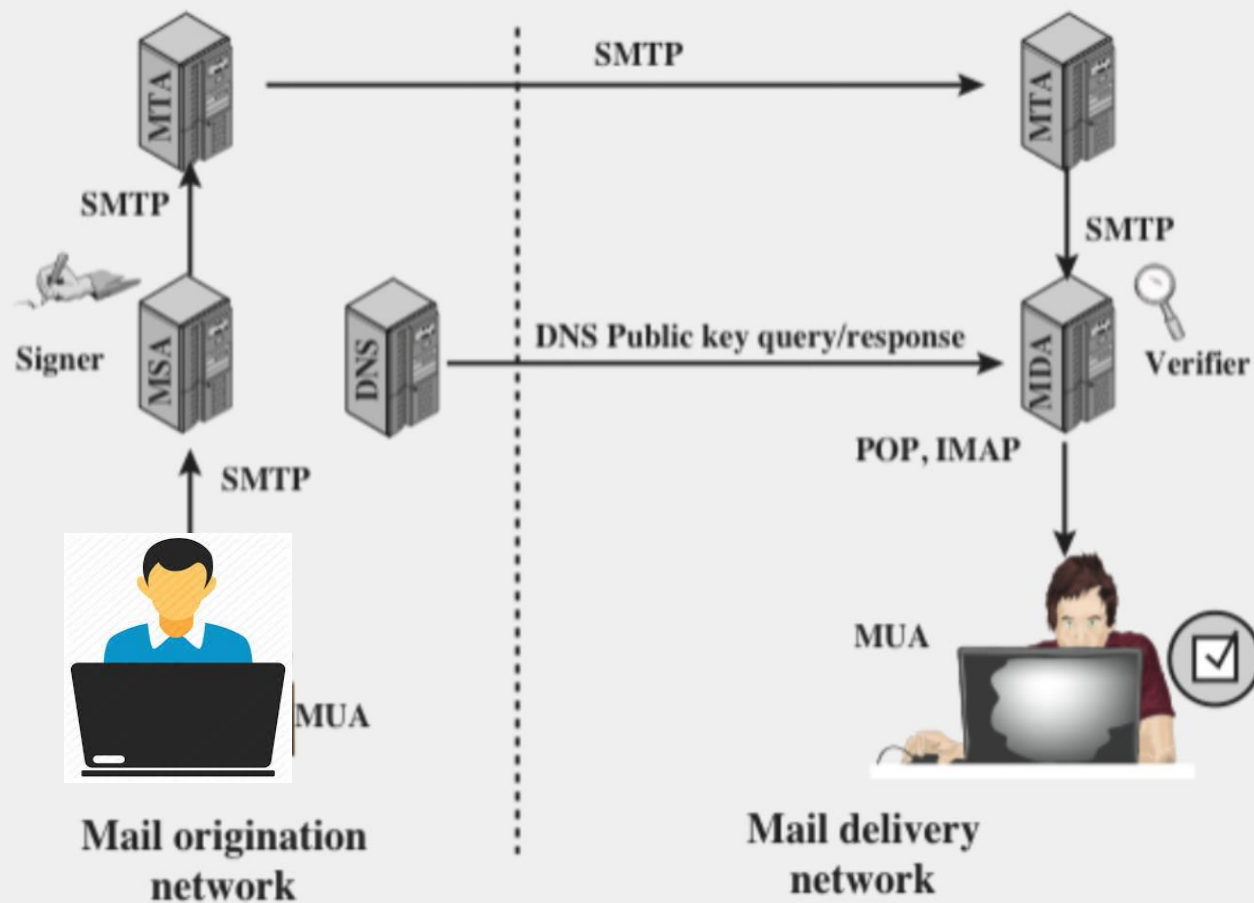
E-mail Threats

- RFC 4684 (*Analysis of Threats Motivating DomainKeys Identified Mail*)

- ▬ Describes the threats being addressed by DKIM in terms of the characteristics, capabilities, and location of potential attackers

- Characterized on three levels of threat:





DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent

Figure 8.5 Simple Example of DKIM Deployment

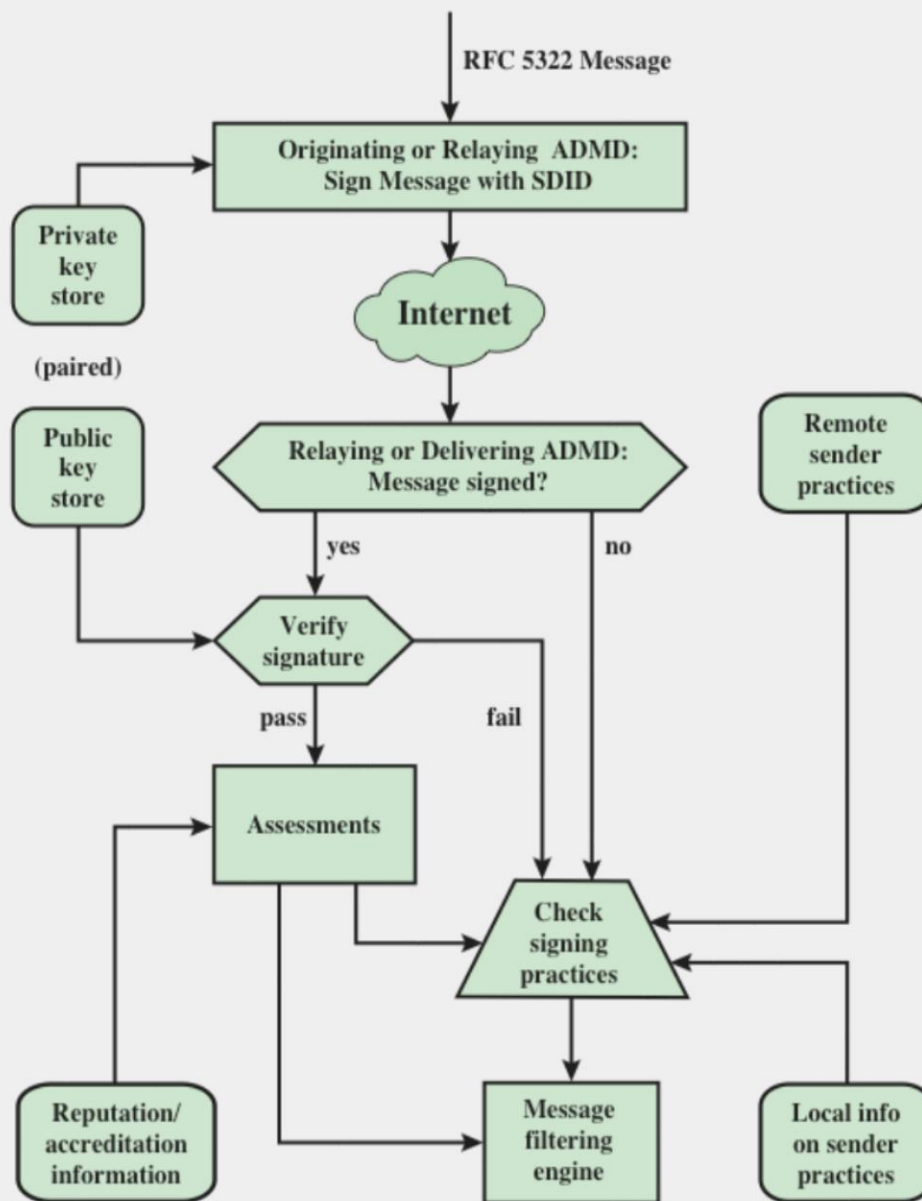


Figure 8.6 DKIM Functional Flow

Recommended Web Sites

- ❑ PGP home page: www.pgp.com
- ❑ MIT distribution site for PGP
- ❑ S/MIME Charter
- ❑ S/MIME Central: RSA Inc.'s Web Site

يا ذا الامن والامان

پایان

