An Exploration of S/MIME Error Conditions in Popular Mail User Agent Interfaces

Bachelor Arbeit

Maria Sigal

Arbeitsgruppe Sichere Identität
Fachbereich Mathematik und Informatik
Freie Universität Berlin

5. April 2018

Freie Universität Berlin

S/MIME

A set of standards for secure email messaging defined by IETF.
Uses:

1. digital signatures
2. encryption

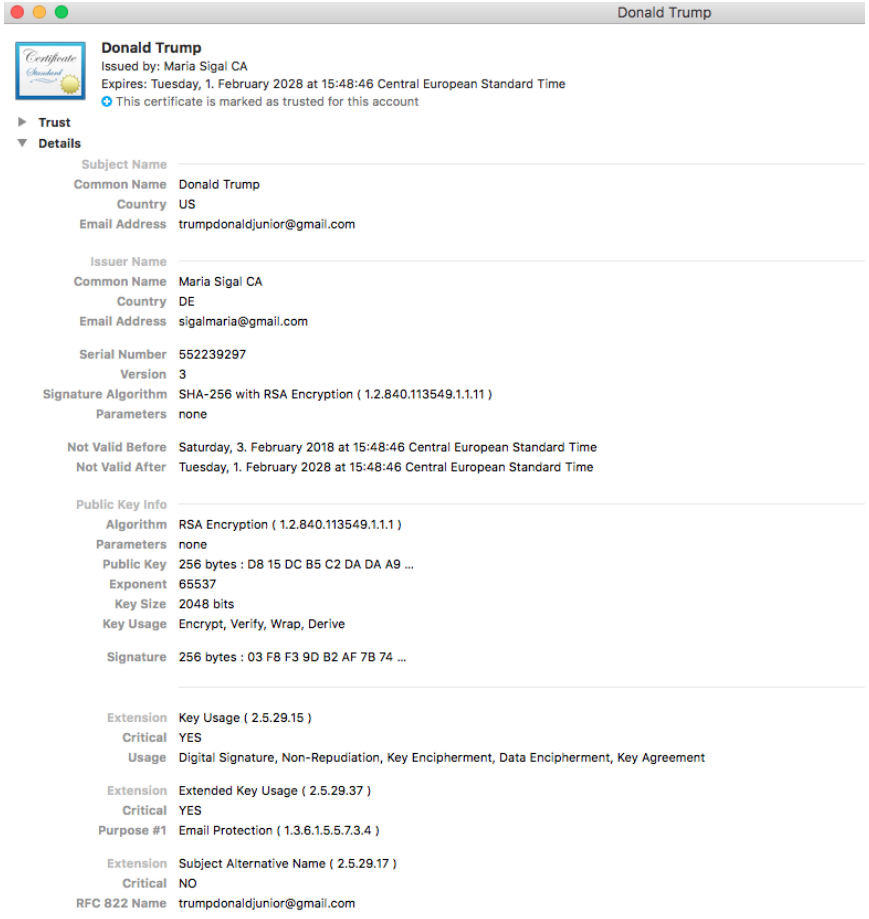
S/MIME

S/MIME provides:

1. authentication
2. message integrity
3. non-repudiation of origin
4. data confidentiality

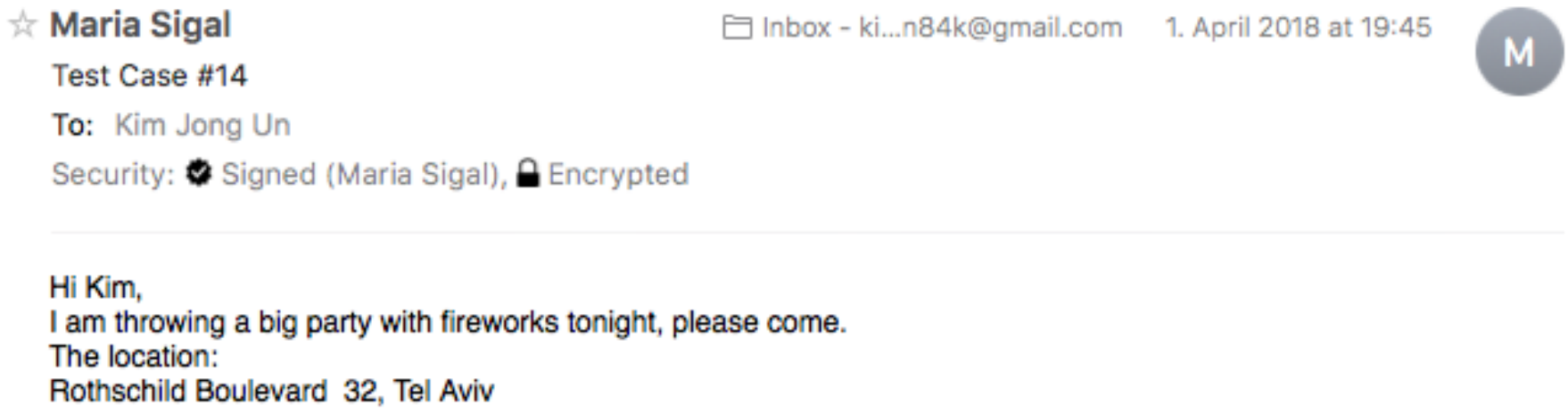
S/MIME Certificates

Bindings between public key and identities



S/MIME in Mail on MacOs

for example:



Errors in Implementation

1. the programm has to be vulnerability-free
2. developer do implementation mistakes

find exploit to :

1. forge a signature on an arbitrary email message
2. obtain decrypted content.
3. disrupt email client services.

Methods:

create complex email message structures:

1. manipulating S/MIME objects.
2. manipulating other objects related to S/MIME such as MIME, CMS.
3. applying a different combination of security operations.

MIME

The Multipurpose Internet Mail Extensions (MIME) is RFC Internet standard RFC which defines the data format of emails.

1. textual message bodies in character set other than US-ASCII.
2. an extensible set of different formats for non-textual message bodies like images, application pro- grams, videos.
3. messages bodies with multiple parts.
4. textual header information in character sets other than US-ASCII

Multipart alternative

```
From: Maria Sigal <sigalmaria@gmail.com>
Content-Type: multipart/alternative;
    boundary="Apple-Mail=_0986B0D4-DE68-4489-80E6-DC7266BE5142"
Mime-Version: 1.0 (Mac OS X Mail 10.3 \(3273\))
Subject: Html
X-Universally-Unique-Identifier: B71EE87B-E4F0-4A2F-8EFF-ED6050BB6439
Message-Id: <8DBCBFC9-829D-4690-AB17-ECAE09280F24@gmail.com>
Date: Wed, 4 Apr 2018 14:48:36 +0200
To: Maria Sigal <sigalmaria@gmail.com>


--Apple-Mail=_0986B0D4-DE68-4489-80E6-DC7266BE5142
Content-Transfer-Encoding: 7bit
Content-Type: text/plain;
    charset=us-ascii

Kishuf
Ze kishuf



--Apple-Mail=_0986B0D4-DE68-4489-80E6-DC7266BE5142
Content-Transfer-Encoding: 7bit
Content-Type: text/html;
    charset=us-ascii

<html><body style="word-wrap: break-word; -webkit-nbsp-mode: space; -webkit-line-break: after-white-
space;" class="">Kishuf <div class="">Ze<font color="#9929bd" class=""> kishuf</font> </
div><div class=""><br class=""></div><div class=""><br class=""></div></body></html>
--Apple-Mail=_0986B0D4-DE68-4489-80E6-DC7266BE5142--
```

Multipart attachment

```
Mime-Version: 1.0 (Mac OS X Mail 10.3 \(3273\))
Subject: eazzzzzz
Message-Id: <D76AEEF0-2999-4950-BF51-ED565E53BCCC@gmail.com>
Date: Wed, 4 Apr 2018 14:54:59 +0200
To: Maria Sigal <sigalmaria@gmail.com>
X-Mailer: Apple Mail (2.3273)


--Apple-Mail=_A1429141-F66C-4576-B5CB-0264A7882656
Content-Transfer-Encoding: 7bit
Content-Type: text/plain;
    charset=us-ascii

Hi
See the attached image.


--Apple-Mail=_A1429141-F66C-4576-B5CB-0264A7882656
Content-Type: multipart/related;
    type="text/html";
    boundary="Apple-Mail=_3EB51DA6-DA14-495D-92B6-B76D4B55DBDB"


--Apple-Mail=_3EB51DA6-DA14-495D-92B6-B76D4B55DBDB
Content-Transfer-Encoding: 7bit
Content-Type: text/html;
    charset=us-ascii

<html><head><meta http-equiv="Content-Type" content="text/html charset=us-ascii"></head><body
style="word-wrap: break-word; -webkit-nbsp-mode: space; -webkit-line-break: after-white-space;"
class="">Hi<div class="">See the attached image. </div><div class=""><br class=""></div><div
class=""><img apple-inline="yes" id="C6129153-8846-4139-8CA5-63E3334C5C89" src="cid:326B0619-3DDB-4F82-
B9A7-A01BE75E874F" class=""></div></body></html>
--Apple-Mail=_3EB51DA6-DA14-495D-92B6-B76D4B55DBDB
Content-Transfer-Encoding: base64
Content-Disposition: inline;
    filename=nickiminaj.jpeg
Content-Type: image/jpeg;
    name="nickiminaj.jpeg"
Content-Id: <326B0619-3DDB-4F82-B9A7-A01BE75E874F>
```

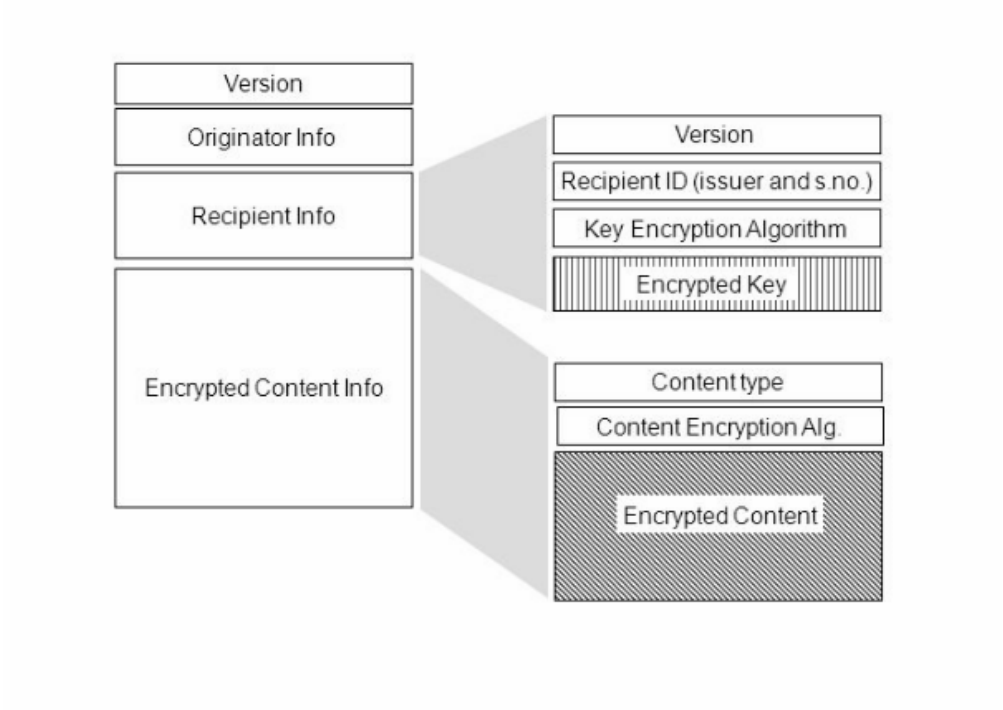

```
/9j/4AAQSkZJRgABAQAASABIAAD/wAARCAFAAO8DASIAAhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAA
AAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKB
kaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZn
aGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT
1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcI
CQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHBCSMzUvAV
YnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkNERUZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6
goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3uLm6wsPExcbHyMnK0tPU1dbX2Nna4uPk
5ebn6Onq8vP09fb3+Pn6/9sAQwACAgICAgIDAgIDBQMDAwUGBQUFBQYIBgYGBgYICggICAgICAoK
CgoKCgoKDAwMDAwMDg4ODg4PDw8PDw8PDw8P/9sAQwECAwMEBAQHBAQHEAsJCxAQEBAQEBAQEBAQ
EBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQ/90ABAAP/9oADAMBAAIRAxEA
PwD88fjQNnidJv7yg/rX2n4RFze/D7ScnCCMYGa+KPjKHOuRB+DsFfc/w1sZrr4baY0ny5jAGOuM
V4NCOs0fcVnrFkFzp0rRQShsBTjA5NfA/wAcrI23ijUFPdQf51+mEFjaRokbgttPHua/Pj9ouwjt
/Gd4sefmjBOfrXp0tJWPKxWtNs8D8JRunh+SXPBbH619g/B1GkiQL2Qf+givkbwkly3hyYRoWjV+
T6c19YfBi4AcRZ+baP8A0GlRfuz9TmXX0/Q+kLhC1pl8EivjP41eXD4e1a+tprtJIrmMEhk
```

CMS

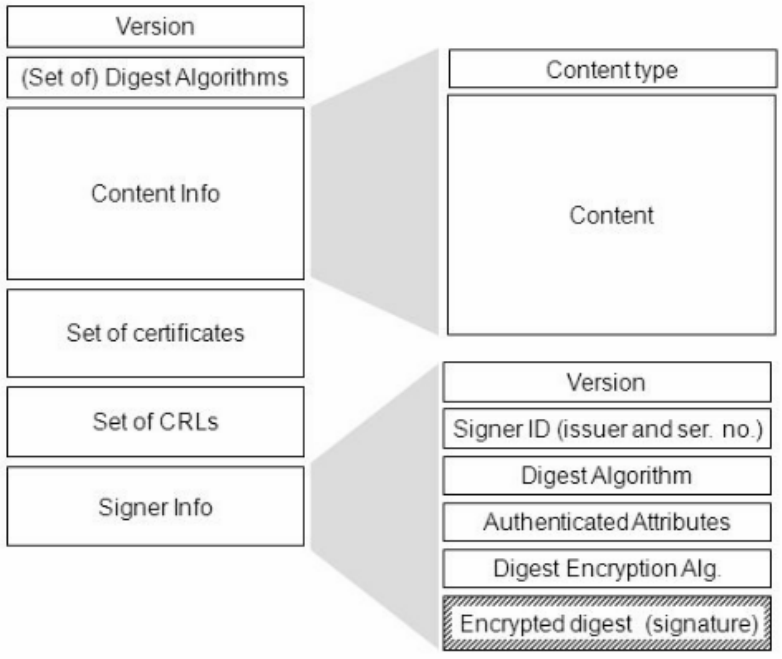
cryptographic message syntax(CMS)

1. IETF standard for cryptographically protected messages.
2. can sign and encrypt arbitrary message content.
3. allows multiple encapsulations.

CMS EnvelopedData



CMS SignedData



nested CMS

1. any combination of cryptographic operations could be applied to the message.
2. signBy(Maria) →signBy(Donald) →encrypt
3. encrypt→encrypt →sign
4. etc.

encrypted message with S/MIME

```
Content-Type: application/pkcs7-mime; name="smime.p7m"; smime-type=enveloped-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: S/MIME Encrypted Message

MIAGCSqGSIb3DQEHA6CAMIACAQAxggFvMIIBawIBADBTMEsxFzAVBgNVBAMMDk1hcmlhIFNpZ2Fs
IENBMQswCQYDVQQGEwJERTEjMCEGCSqGSIb3DQEJARYUc2lnYWxtYXJpYUBnbWFpbC5jb20CBDRn
XYEwDQYJKoZIhvcNAQEBBQAEggEAdkYz5GkttFzLJzbJRh28x2gQKEWuc/fo8ljUNHW6jech3xv5
bcOGcMqNVwHRaYAovu0yeSgviAN5TtAkSAMmBK1bZbsY4QmX3qnvJHki/ZkCAfRvKfZ9W9My/BRH
/gSur0MvX+6OnF0Ay0owO3EFyVd8tYJI4uz2GCj901b7CLEJgclR2ONZWnDLGO1WsC+ySyqfvzY8
BIF/E3o4edMHeaV1D031GnVKrdkUDSjzAwH3tThkfRniOKPiCF4x5i6lkVouTgBN30dCio+SQeKK
D+7qFDB+50eLrFC+mUE7XQs/88BYD16sYh9SLWTUEHDYtxftVCo0BExcUpfm3dNZCzCABgkqhkiG
9w0BBwEwHQYJYIZIAWUDBAEqBBBaiHgD7q8xQA50GBUTR96poIAEggPoNImt9M88YNJwXqUKMdny
4rz8wylQBpFgF+KZI5EtBwAqqVhYCbS8nK+1IixVDDntFLDlCOHDK9ZbT1lha22DUpeE2KSBQDCX
fTlP2JjTiNksWlbo887hRWhNqYj1tpFV029g3Ms+t0aK0nzFBy+J0RSUXvCUoImbbPLmPA9ZAaAX
```

signed message with S/MIME

```
Return-Path: <trumpdonaldjunior@gmail.com>
Received: from wlan-141-23-162-91.tubit.tu-berlin.de (wlan-141-23-162-91.tubit.tu-berlin.de.
[141.23.162.91])
        by smtp.gmail.com with ESMTPSA id r16sm3443510edb.22.2018.04.04.06.42.26
        for <kimjongun84k@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Wed, 04 Apr 2018 06:42:26 -0700 (PDT)
Date: Wed, 4 Apr 2018 15:42:24 +0200 (CEST)
From: trumpdonaldjunior@gmail.com
To: kimjongun84k@gmail.com
Message-ID: <1272753974.3.1522849344789@gmail.com>
Subject: Test Case #01
MIME-Version: 1.0
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=sha-256;
    boundary="----=_Part_1_196025267.1522849344744"

------=_Part_1_196025267.1522849344744
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

Something blowing in my head,
Winds of ice that soon will spread
------=_Part_1_196025267.1522849344744
Content-Type: application/pkcs7-signature; name=smime.p7s; smime-type=signed-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIAGCSqGSIb3DQEHAqCAMIACAQExDzANBglghkgBZQMEAgEFADCABgkqhkiG9w0BBwEAAKCAMIID
azCCAlOgAwIBAgIEIOqAwTANBgkqhkiG9w0BAQsFADBLMRcwFQYDVQQDDA5NYXJpYSBTaWdhbCBD
QTELMAkGA1UEBhMCREUxIzAhBgkqhkiG9w0BCQEWFHNpZ2FsbWFyaWFAZ21haWwuY29tMB4XDTE4
MDIwMzE0NDg0NloXDTI4MDIwMTE0NDg0NlowUDEVMBMGA1UEAwwMRG9uYWxkIFRydW1wMQswCQYD
VQQGEwJVUzEqMCgGCSqGSIb3DQEJARYbdHJ1bXBkb25hbGRqdW5pb3JAZ21haWwuY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2BXctcLa2qnqv+aORZ2+FdtEFtZc33bu1UOaiawk
N7TYT6btbKcf3uwLjFPZdlyLgD0LZIs66IWA52PoMOYalMo8ZQt725mIAVq/pfAGfCMqf1nvn/8g
kgTwyJyCLZlNSbe4vyD6LtwKIhjHts4zj3qJ1MBXkwDJ1VpdkhWi7jt/ucUOPYWxIe09VutCC0R9
TwLyoKmXC+5XdlEgOVHZocVUcGtlznOtH41StDTAocPB6CbKCed1HjH4xncc7u7yZ+oTgTL2n0dC
xsAmbA+prBBydbWRLXqZ58jRtztjOZa+UuOD1yhcooxFx3q+wPZi6Tou4wNihJJQap76fqVLUQID
AQABo1IwUDAOBgNVHQ8BAf8EBAMCA/gwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwQwJgYDVR0RBB8w
HYEbdHJ1bXBkb25hbGRqdW5pb3JAZ21haWwuY29tMA0GCSqGSIb3DQEBCwUAA4IBAQAD+POdsq97
dLayz3zQvJz5qpJ+/wdH374zfnpldFDFRz/JUfpNeQMZKcyRheWOB9tV9P+ehHSQtrkz2a8wmojx
4SvjFn1HnFjwEky14evfVpGokysV6fdSPilHhT/em86Z+3prFvt6LXnrhSRaHZooUEWJzXIo5+Ii
pleted successfully with 3 warnings in 9s 332ms (2 minutes ago)
```

S/MIME could be also nested

According to the standard, each individual layer of CMS is wrapped with MIME. For example, for sign →encrypt

1. a MIME entity of type text/plain is created.
2. the MIME entity is processed to the CMS SignedData object.
3. the CMS SignedData is encoded with base64 and wrapped with S/MIME.
4. S/MIME message is processed to the CMS EnvelopedData object.
5. the CMS EnvelopedData is encoded with base64 and wrapped with S/MIME.

Test cases

Test Suite Name	Test Suite Id	Test Case Id
S/MIME basic functionality	101	1, 2, 3
S/MIME sign & encrypt flaw	102	33, 34, 36,38
S/MIME standards violation	103	25, 26
S/MIME encapsulation	104	11, 12, 13, 14, 27, 33, 34,36,37
CMS encapsulation	105	18, 19, 20, 21 ,30, 31, 32
S/MIME as an email attachment	106	16, 17, 22,
S/MIME with "multipart/alternative" messages	107	4,5 ,6, 10, 15
S/MIME with "multipart/mixed"	108	7, 8, 9 , 23, 24, 28
S/MIME with multiple certificates	109	11, 12,13 ,14

S/MIME test tool development

1. importing of sender and recipient certificates.
2. generation of email messages according to propertis defined.
3. sending generated email messages to the recipient.
4. saving the sent messages as a text file.

S/MIME test tool development

1. jdk 1.8
2. bcmail-jdk15on library of BouncyCastle
3. JavaMail API version 1.6.0.
4. java.security

Tested Email Clients

1. Mail on IOS 11.2.5
2. Thunderbird 52.6.0 on macOs Siere 10.12.16
3. Mail 10.03 on macOs Siere 10.12.16

running the tests

```
gatter:smimetesting berutiel$ java -jar target/SmimeTest.jar -prop "config/config.properties" -test 14
Connecting to smtp server
mail.smtp.host: smtp.gmail.com
mail.smtp.port: 587
Executing Test Case 14

The following  message sent:

[

[Date: Fri, 23 Feb 2018 14:02:42 +0100 (CET)
From: trumpdonaldjunior@gmail.com
To: kimjongun84k@gmail.com
Message-ID: <1564078808.5.1519390962772@gmail.com>
Subject: Test Case #14
MIME-Version: 1.0
Content-Type: application/pkcs7-mime; name=smime.p7m; smime-type=signed-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHAqCAMIACAQExDzANBglghkgBZQMEAgEFADCABgkqhkiG9w0BBwGggCSABIID
6ENvbnRlbnQtVHlwZTogYXBwbGljYXRpb24vcGtjczctbWltZTsgbmFtZT0ic21pbWUucDdtIjsg
c21pbWUtdHlwZT1lbnZlbG9wZWQtZGF0YQ0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogYmFz
ZTY0DQpDb250ZW50LURpc3Bvc2l0aW9uOiBhdHRhY2htZW50OyBmaWxlbmFtZT0ic21pbWUucDdt
Ig0KQ29udGVudC1EZXNjcmlwdGlvbjogUy9NSU1FIEVuY3J5cHRlZCBNZXNzYWdlDQoNCk1JQUdD
U3FHU0liM0RRRUhBNkNBTUlBQ0FRQXhnZ0Z2TUlJQmF3SUJBREJUTUVzeEZ6QVZCZ05WQkFNTURr
MWhjbWxoSUZOcFoyRnMNCklFTkJNUXN3Q1FZRFZRUUdFd0pFUlRFak1DRUdDU3FHU0liM0RRRUpB
UllVYzJsbllXeHRZWEpwWVVCbmJXRnBiQzVqYjIwQ0JEUm4NClhZRXdEUVlKS29aSWh2Y05BUUVC
QlFBRWdnRUFyaEFBOUZVaXdvMWh1MnFHTy9xZ3NJV3EzSWE1bVVSVldobll5TFV3VzJlNlN4bDMN
Ck1EL3JkcEVNWFcyMkFGSzlrRzkrcW9VZ0Q1WEdSOFZaWUR3ZkNVNDh0YTNhTGZhZ2VFdU5HUlZy
YnZITXl0Y1pYOXFrSE1ySk40Ly8NCnZZYjBBVTJQYWZ1SHpsVStidjhWeEg3TXVrWWl3ZytPQlZE
cnJpU2tWV1JtNGR3MFlKSkZVelkwdWtGQ2wxUHJEQXJRRFlxbVA0ZmwNCmRhT1VhTEhsZytxM2FE
UklQQnFMUGJuV2lLRkZMdzJXNk1jb2d5aUlXNFJSaHNpNnBGR2xVKzladG94SDJmRDFtcm03Umk2
Q3V2cjINClhQNE96a3I1VHJLVzliZ0VyaElTYW8yVFo2cmh1SjVyUms3RXlmbEE4cmFuN1QwaGE5
OFphTEdkUjhGV1FJQ2hqVENBQmdrcWhraUcNCjl3MEJCd0V3SFFZSllJWklBV1VEQkFFcUJCRFBN
TWpwcXJiVXFrYTJpMHJNQlcyRG9JQUVnZ1BveUJ2Wk9Ba0a2ZtSjR0a2hSdkU1UVQNCnlOb1h1UTAz
YzBwZ2gzdmszVXNlRnNqZURqTzlKOXFwdUw3eWU3bnZkaVBDTFN1c3FNbW8rTk91SjFpZ1JLU3Bk
YmVhbElNWDRjUTANCmdBZU5QR2ozdSt1VjBqRERrT0FjckdONE9iY3IzUXoyc0gzWDY4bVJZV2hW
S0pYblRSQlQ5dVM3SmpzYk5DdmZsVEkrOWNiMFZMeGgEggPoDQprczhBNjcwaWp6eWN5ZzNURjhV
bStlU3hVbC9RRUFTV0RteGh0UFFQYThuU3VBZzlPMm45cGtIcmo0THA4cGoyNE5HU2YwMDBXcnJB
DQpJY2c1aTJuT2k3OXRWc2VneGtLOU1qVGdWa1NYRS9BQ0xpUmwwVGVBSVJqOWV2dXA1UDNIQTV3
dm11UVdNamNIRXBmV29nWlhRdTV0DQpWWDErdVFveXprYmtuUHJ3d3VBSVBrNDBmd3dvckhubGhH
Y1VGOHVBYVVKUW1BdHV4aXJVREpJNFlINTdBTEtEK2NOYnRqaE1CYkloDQphK0NEazI2bldSeFFr
bmdZcHh4MjgyckJWUEZIMjMwb3BXN1Q0SHNxOGVPZ3RhUXJCdDJXN1FLcWc0R2szOVBhZS84a0hp
UDdEbFdMDQorb1RuWXYyMG9KZDZLWUhwU0ZRQzFpMzA4YzllWWR6emJteFliZmtwQjhhR1ZNQTQ4
T2ZkUjlZRk1KbzZtVGUzM1RlVmVFTEt0K1NaDQpaZC9yeTRZTCttU3YxWlQrU0hWa0JSZVJFQ0Zw
```

SMIMETest is configurable to run with arbitrary .p12, .cer certificates, sender an

Results

36 out of 111 tests failed.

signed S/MIME as an email attachtment 1

We sent the following message:

1. a MIME entity of type text/plain with some text is created and signed with S/MIME multipart/signedformat.
2. another MIME entity of type text/plain with some text is created.
3. an email message of type multipart/mixed is created.
4. a MIME entity from step 2 is appended to the message from step 3.
5. a MIME entity from step 1 is appended as message/rfc822 (email attachment) to message from step 3

Output in Mail MacOs

☆ **Donald Trump** Inbox - ki...n84k@gmail.com 22:20

Test Case #16

To: Kim Jong Un

Update on location:
Franz Merhing Platz 3, Berlin

Nada
From: trumpdonaldjunior@gmail.com
Subject: **signedMessageForAttachment**
Date: 3. April 2018 at 22:20:13 GMT+2
To: kimjongun84k@gmail.com

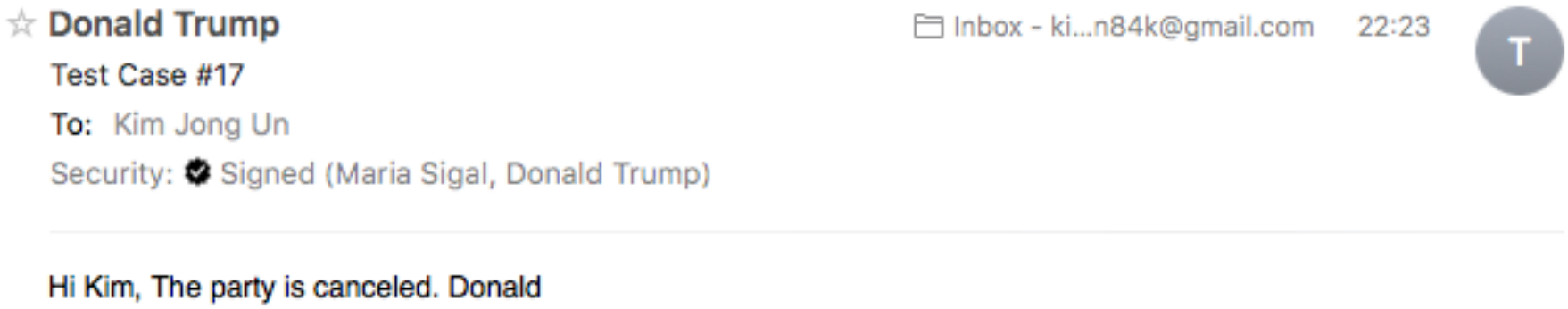
Hi Kim,
I am throwing a big party with fireworks tonight, please come.
The location:
Rothschild Boulevard 32, Tel Aviv
Donald Trump

signed S/MIME as an email attachtment 2

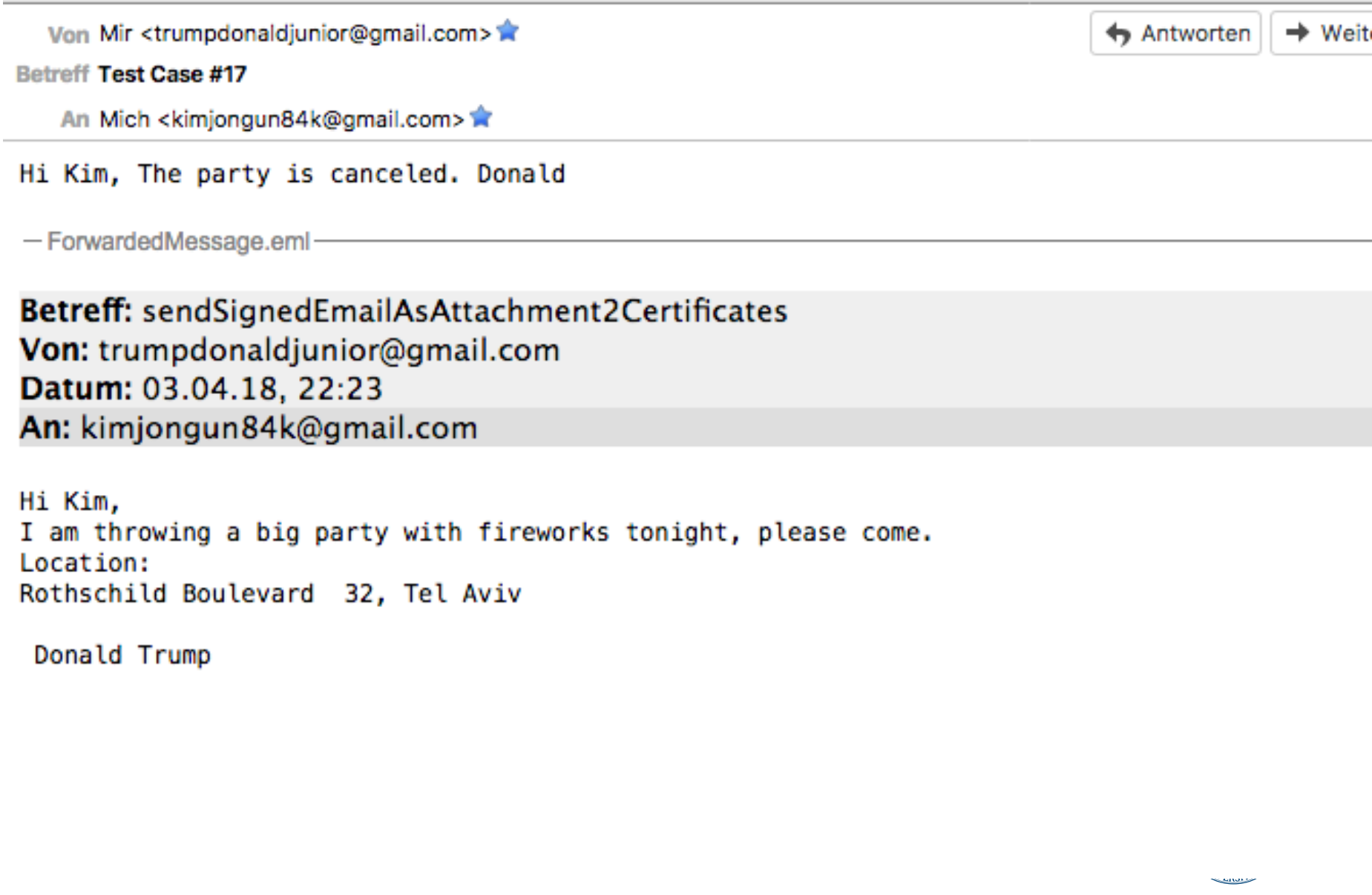
Now we did aditional manipulations:

1. the external body part of type text/html ending with the tag
2. the external body part was signed by Maria Sigal.
3. email message is spoofed to make it look coming from Donal Trump

Output in Mail MacOs



Output in Thunderbird MacOs

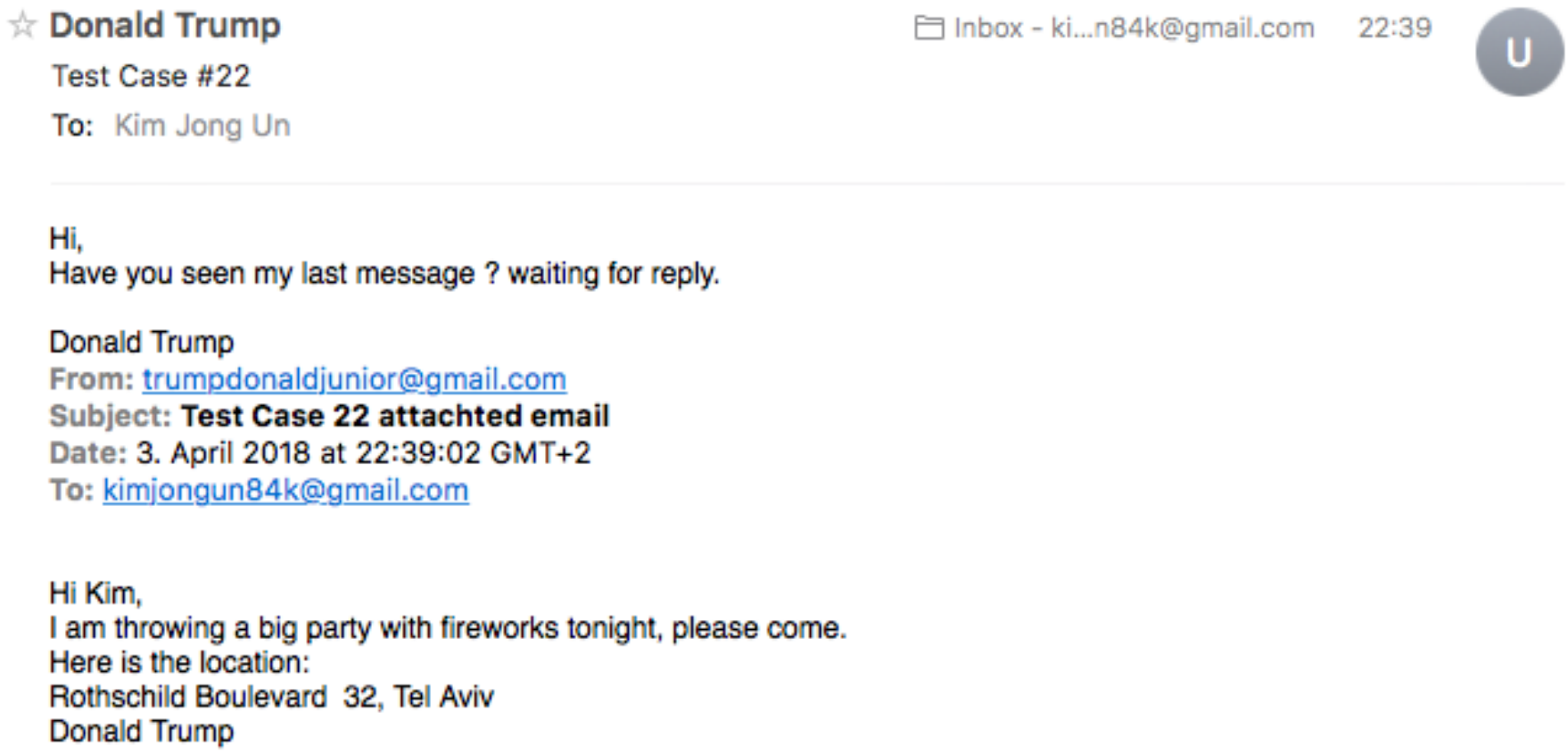


encrypted S/MIME as an email attachtment

1. the external mesage has some text
2. the email message has an encrypted email message as attachment

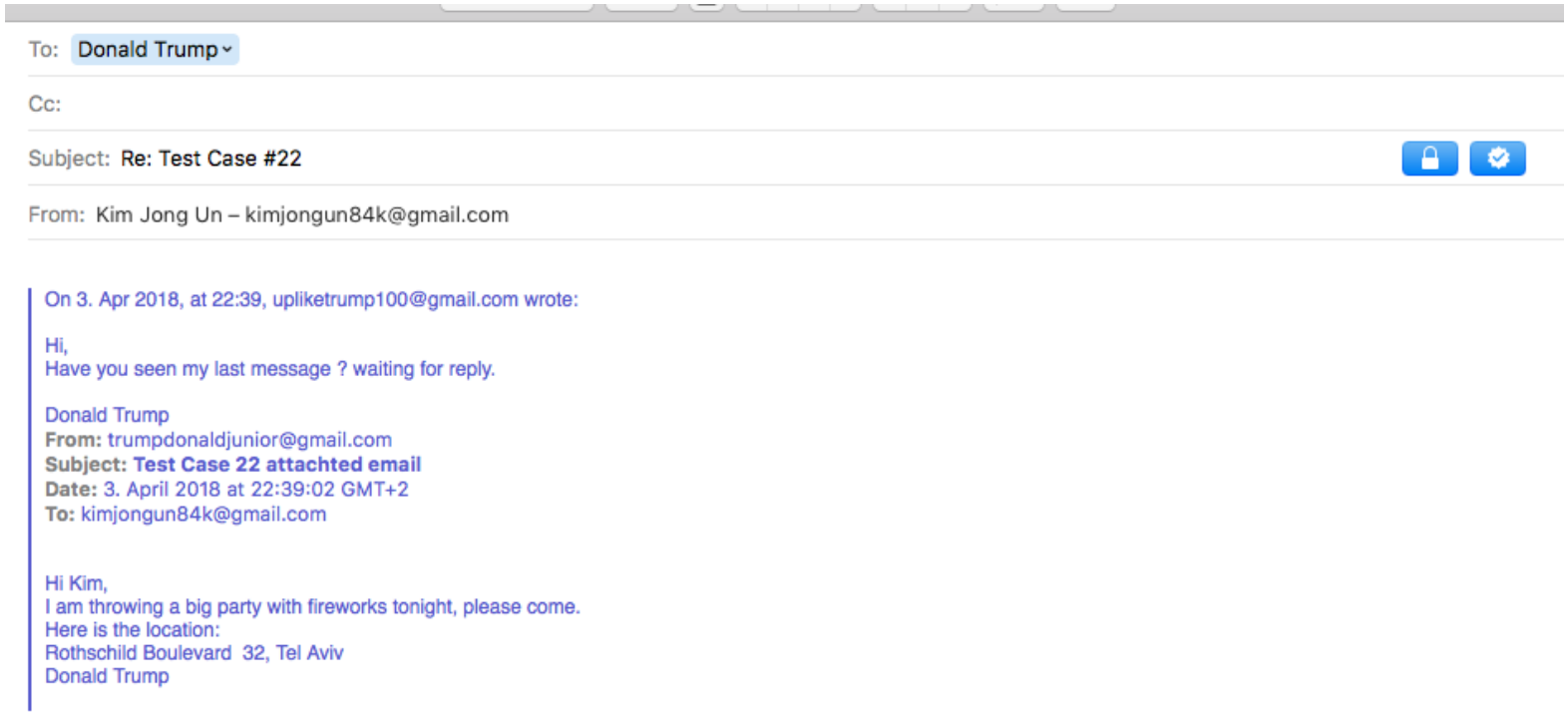
Mail MacOs

no indication for encryption performed.



Mail MacOs

The email attachtment is included in the reply message.


To: Donald Trump

Cc:

Subject: Re: Test Case #22

From: Kim Jong Un – kimjongun84k@gmail.com

On 3. Apr 2018, at 22:39, upliketrump100@gmail.com wrote:

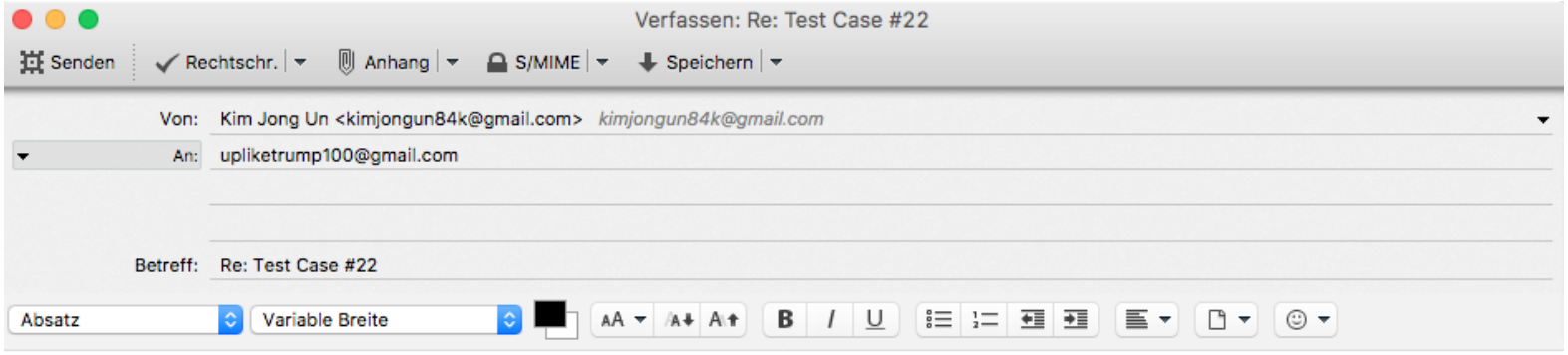
Hi,
Have you seen my last message ? waiting for reply.

Donald Trump
From: trumpdonaldjunior@gmail.com
Subject: **Test Case 22 attachted email**
Date: 3. April 2018 at 22:39:02 GMT+2
To: kimjongun84k@gmail.com

Hi Kim,
I am throwing a big party with fireworks tonight, please come.
Here is the location:
Rothschild Boulevard 32, Tel Aviv
Donald Trump

Thunderbird MacOs

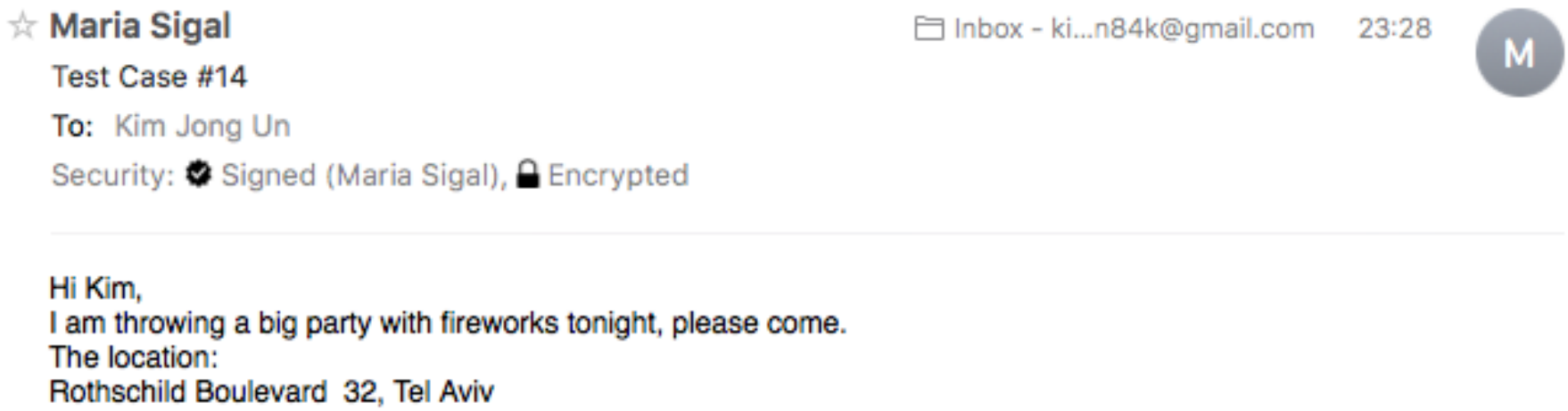
The email attachtment is not included in the reply message.



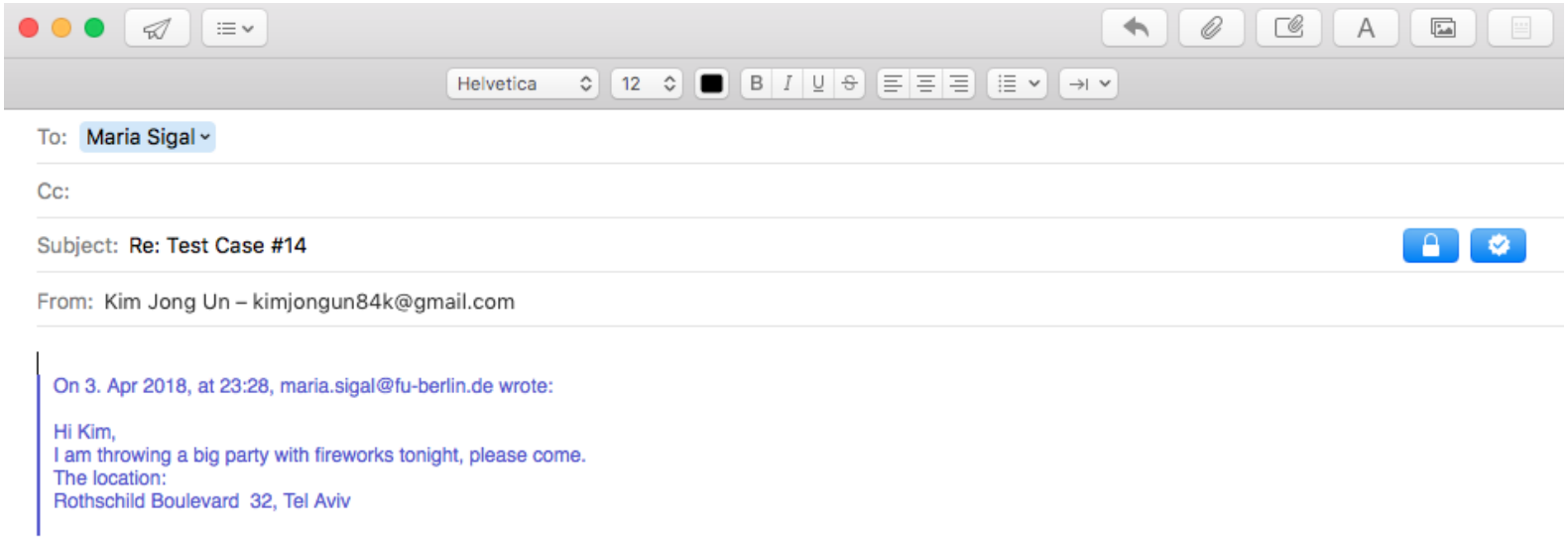
Sign →Encrypt →Sign

1. the MIME entity of type text/plain is signed by Donald Trump
2. The result of 1 is encrypted for Kim
3. the result of 2 is signed by Maria Sigal

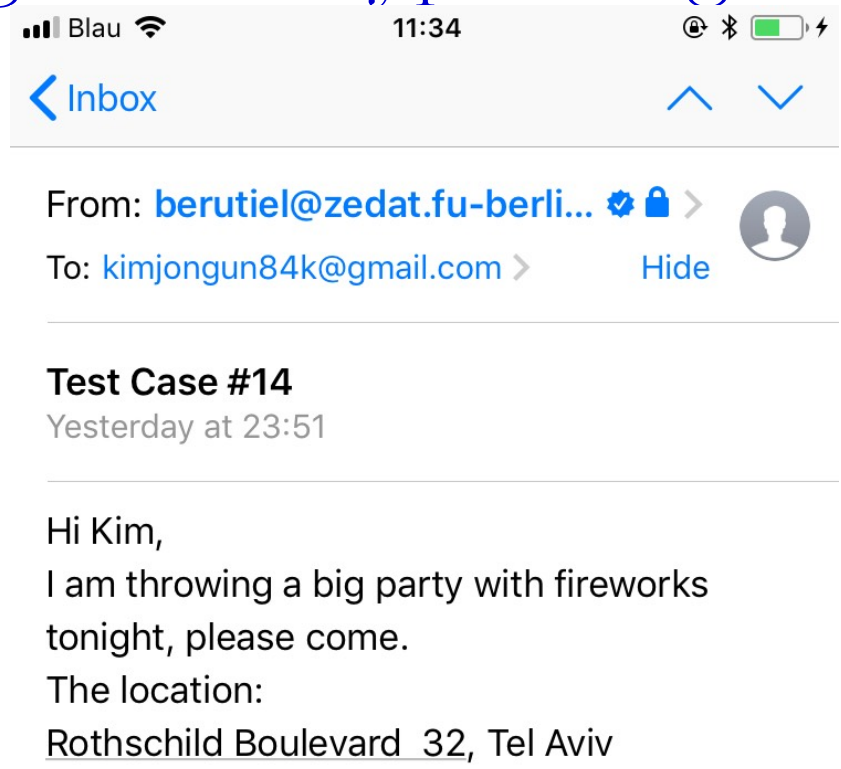
Sign →Encrypt →Sign in Mail MacOs



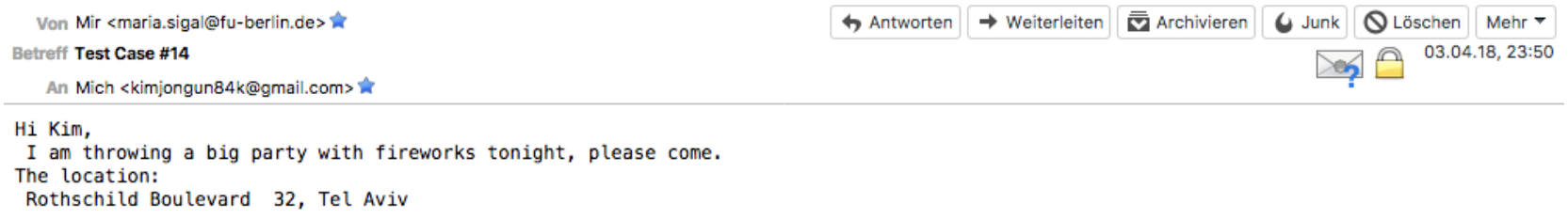
Mail MacOs - reply message



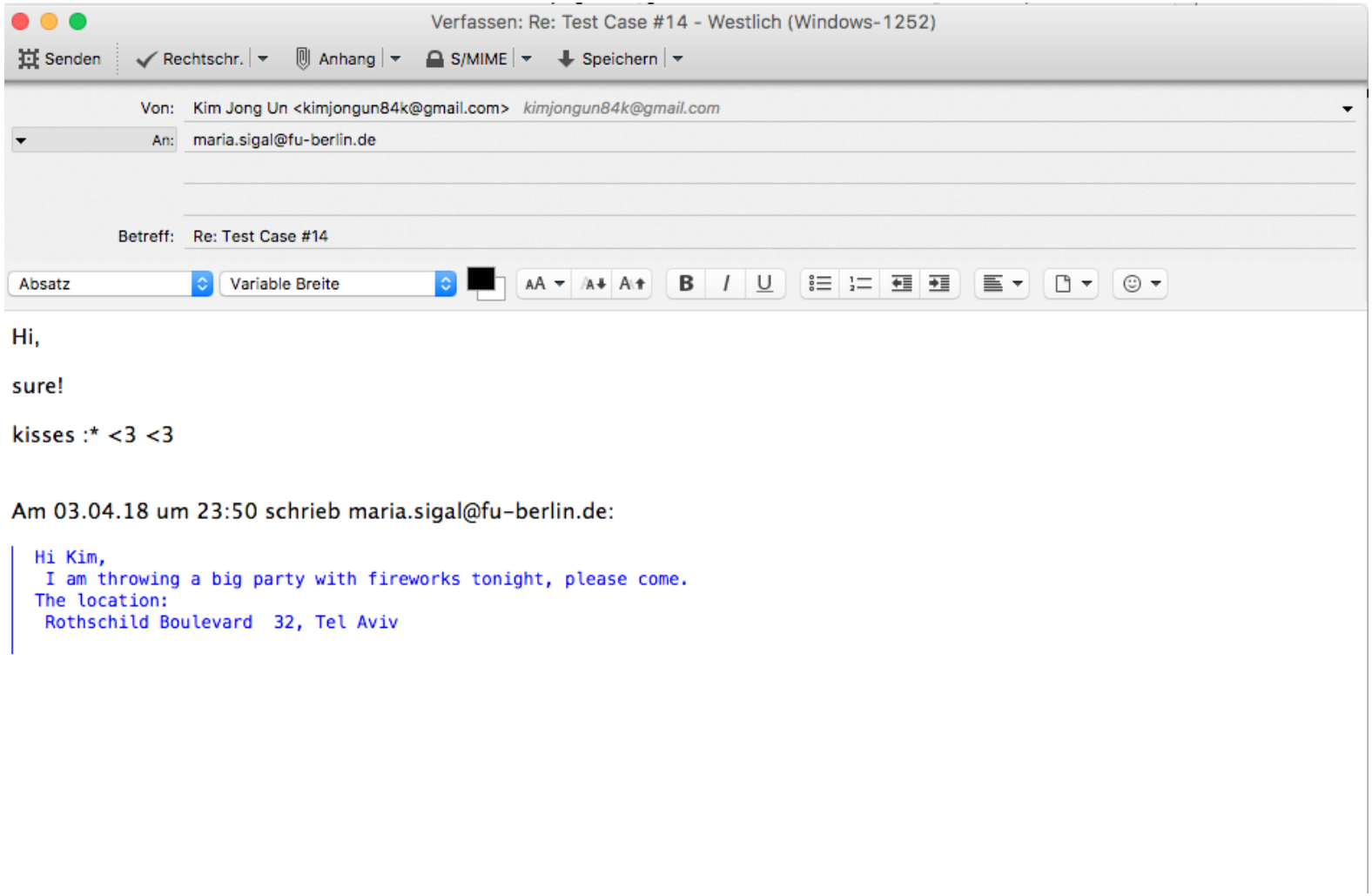
Mail IOS - Sign →Encrypt →Sign



Sign →Encrypt →Sign in Thunderbird MacOs



Thunderbird MacOs - reply message

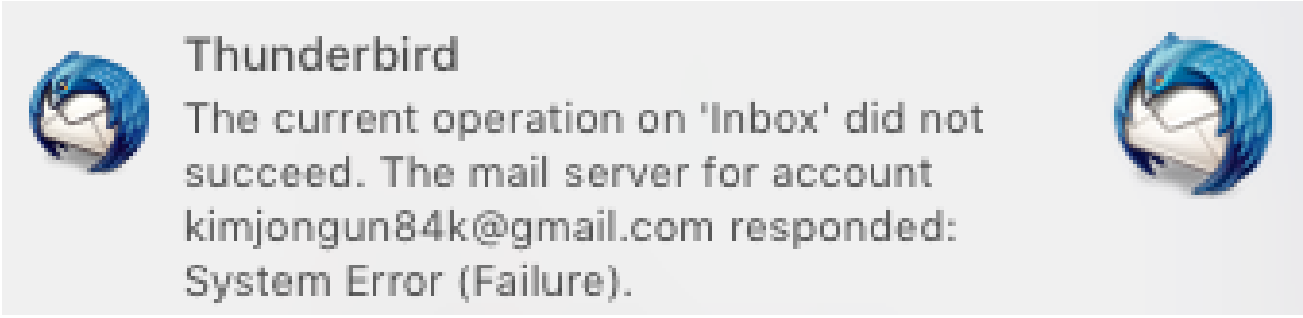


CMS encapsulation

1. the MIME entity is packed in the CMS Enveloped]Data.
2. the CMS EnvelopedData is signed with CMS SingedData by Donald Trump.
3. The result is wrapped with S/MIME.

CMS encapsulation in Thunderbird MacOs

Messages are not downloaded from the server.



CMS encapsulation in Mail IOS

Denial-of-service - any messages later sent to the recipient also not downloaded.

Surreptitious Forwarding Attack

$$A \rightarrow B\{\{"sales\ strategy\ "\}^a\}^B$$
$$B \rightarrow C\{\{"sales\ strategy\ "\}^a\}^C$$

Encrypt-and-Sign Attack

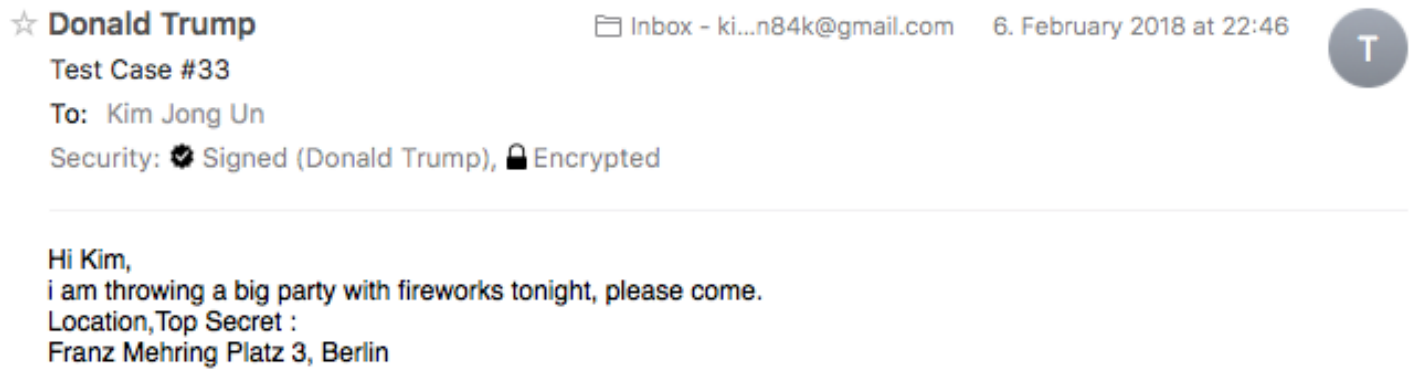
$$A \rightarrow B\{\{\text{"}new\ invention\ \text{"}\}^B\}^a$$
$$B \rightarrow C\{\{\text{"}new\ invention\ \text{"}\}^B\}^c$$

Repairs

1. Sign the recipient's name into the plaintext
2. Encrypt the sender's name into the plaintext
3. Incorporate both names
4. Sign the signed and encrypted message again
5. Encrypt the signed ciphertext again

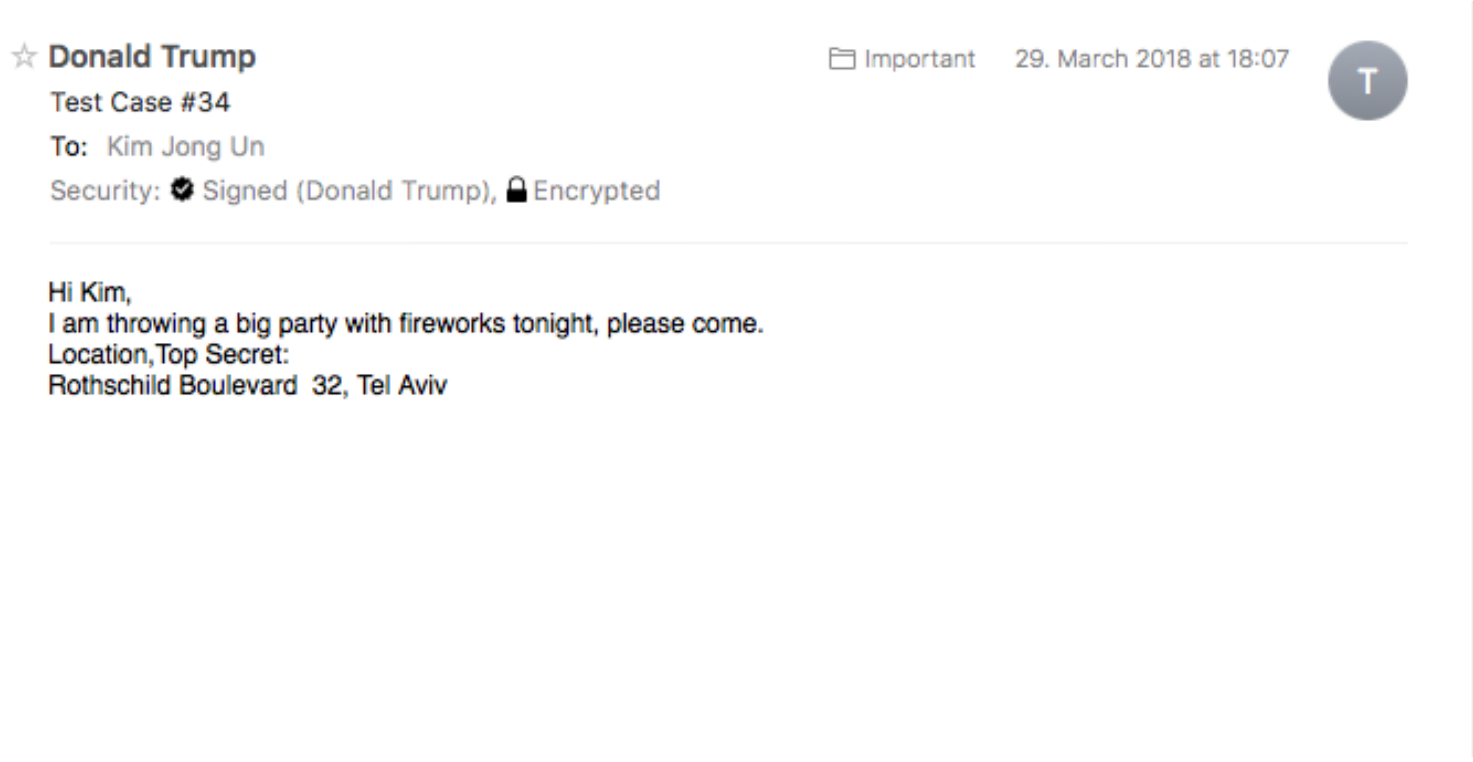
Sign →Encrypt →Sign

Not supported. The same output as with the sign-then-encrypt message.



Encrypt →Sign→Encypt

Not supported. The same output as with the sign-then-encrypt message.



Danke