RIPEM Message and File Formats

Mark Riordan

4 May 1993

This document describes the syntax of messages produced by RIPEM, and of files maintained by RIPEM.

Format Standards Followed by RIPEM

RIPEM messages generally follow the format described in Internet RFC 1421. (In non-PEM mode, some of the fields are different, to account for the lack of certificates in non-PEM mode.) MIME extensions are described in the Internet Engineering Task Force Draft entitled "MIME-PEM Interaction" (`draft-ietf-pem-mime-02.txt`).

Where applicable, RIPEM databases contain fields in formats conformant with RSA Data Security's Public Key Cryptography Standards. See the documents in the `pkcs` directory on FTP site `rsa.com`.

Messages produced by RIPEM and files maintained by RIPEM are kept entirely in 7-bit ASCII format. Information which is inherently non-ASCII ("binary" data such as the output from DES encryption) is encoded either in ASCII hexadecimal, or in a *uuencode*-like format in which three 8-bit bytes are represented with four ASCII characters. (The details of this encoding, which are not identical to those of the Unix *uuencode* program, are described in RFC 1421.) Complex structured information, such as a public key (which contains both a modulus and a public exponent) is first transformed into a portable binary format before being ASCII-encoded. The portable structured format is called DER encoding (for Distinguished Encoding Rules). Descriptions of DER encoding can be found in documents written by Burt Kaliski and available from the FTP site `rsa.com` in the `pkcs` directory.

Factors Affecting Message Formats

Each RIPEM-encrypted message consists of two fundamental parts: a set of "headers" containing bookkeeping information such as the sender's identity, encryption modes used, etc; and a "body" containing the (usually) encrypted message itself. The precise format of RIPEM message headers depends upon several factors:

- Whether the message is enciphered in "RIPEM mode", which does not support certificates, or "PEM mode", which does.
- Whether the message is encrypted, or just signed.
- Whether MIME ("Multipurpose Internet Mail Extensions") is used. MIME format is generally used only when the message being encrypted is not plain ASCII.

PEM-Mode Messages

We will start by describing RIPEM messages produced in PEM mode. Here is an annotated example. (Annotations are indented.)

```
-----BEGIN PRIVACY-ENHANCED MESSAGE-----
```

All RIPEM messages start with this line.

```
Proc-Type: 4,ENCRYPTED
```

"4" indicates standard Internet RFC 1421 PEM.

The second parameter can be ENCRYPTED, MIC-ONLY, or MIC-CLEAR. The message is encrypted only in the case of ENCRYPTED, but a signature is always computed.

```
Content-Domain: RFC822
```

RFC822 indicates that the message plaintext is in standard email (ASCII-only) form. This is currently the only allowable value for this field.

```
DEK-Info: DES-CBC,401E9139E4867FF7
```

This field is present only for ENCRYPTED messages, and indicates the message data encryption algorithm and mode (always DES-CBC), and the initialization vector in hex.

```
Originator-Certificate:
 MIIBpjCCAUICARYwDQYJKoZIhvcNAQECBQAwTTELMAkGA1UEBhMCVVMxIDAeBgNV
 BAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMRwwGgYDVQQLExNQZXJzb25hIENl
 cnRpZmljYXRlMB4XDTkzMDQxOTIwMDI1MFoXDTk1MDQxOTAwMDAwMFowZDELMAkG
 A1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMRwwGgYD
 VQQLExNQZXJzb25hIENlcnRpZmljYXRlMRUwEwYDVQQDEwxNYXJrIFJpb3JkYW4w
 WTAKBgRVCAEBAgICBgNLADBIAkEylZc/H+pNFRQqHC4abJQV4gTzRuGoXmOFgdeP
 kDshmAB4dAa6qY8ypsLqDFmXfbEInjzwxz8weBHGRnTZwFcrMwIDAQABMA0GCSqG
 SIb3DQEBAgUAA08ABMavdfXztriNQZwk8Ma/YbMOd81sg/bASPXKi2FhmDn2WhdZ
 967PW+ZPYkCDn0JdUikP/41xvKuHhOPDNROvN+Sltgf0aFenF2m8/voX
```

This is the certificate of the sender of the message. It contains the sender's public key. See the section below on certificates.

```
Issuer-Certificate:
 MIIBxjCCAVACBF4AAAMwDQYJKoZIhvcNAQECBQAwXzELMAkGA1UEBhMCVVMxIDAe
 BgNVBAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMS4wLAYDVQQLEyVMb3cgQXNz
 dXJhbmNlIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTkyMTIyMzA4MDAwMFoX
 DTk0MDEwMTA3NTk1OVowTTELMAkGA1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRh
 IFNlY3VyaXR5LCBJbmMuMRwwGgYDVQQLExNQZXJzb25hIENlcnRpZmljYXRlMGkw
 DQYJKoZIhvcNAQEBBQADWAAwVQJOBqoIUA2vV4v9swHWBKiVSHGIZSzdRaSPbV0N
 Zus2d/T2FyvFIaI9BLO5Fkb/IQtOL6pDisJ3Vm81bb6B0Dpj/JzpJLgYvgEL4BaE
 XIDlAgMBAAEwDQYJKoZIhvcNAQECBQADYQCPF1HZAPzWWKSyspFjbUGkmQAWGLtz
 3Zvl1nn3EztPPVtR6GirTpFRa07ov7isHWEdZxGKIwbmFPJuh8pn8tTrSyYfWfD6
 /CHEa04fhZ4jVoAmKmjdgbRTqfraABsBAC8=
```

This is the certificate of the authority that issued and signed the Originator-Certificate. This field is optional. It may be followed by the certificate of the authority that issued *this* certificate, and so on up to the root of the certificate hierarchy. RIPEM does not do this. In fact, there is currently no Internet PEM hierarchy.

```
Key-Info: RSA,
 LookV1eGyPwZJ4sz2Eyf1ak3re3Sti2JeSIIaost1SeW93L3eqcXCAqGz7GBBJfN
 hSziXJDIbNEGGXdm9Zuoc0E=
```

The Key-Info field gives the message key of this message, encrypted under the recipient's public key component. This first occurrence of Key-Info, appearing before the first Recipient-ID-Asymmetric field, is optional and applies to the sender of the message. That is, the value of this field as it appears here is the DES message key encrypted with the sender's public key. This allows the sender to decrypt his own messages and is similar to the sender making himself a recipient of all his messages.

The "RSA" here indicates use of the RSA public key algorithm; there are no other legal values for the first parameter.

```
MIC-Info: RSA-MD5,RSA,
 93KkysZ67I408OZOr6GaimrSez7XUW9ezIWhqtDeXSNNomyeBPrr9EAPDKb52Y97
 KKhSksBlJKaF5J+1KclEihUns91EGUfA
```

MIC-Info gives the message digest of the message, encrypted with the sender's private component. That is, this is the "signature".

The first parameter is the message digest algorithm. RIPEM always uses RSA-MD5 during encryption, but will also recognize RSA-MD2 upon decryption.

The second parameter specifies the public key cipher used to encrypt the digest. This is always RSA.

```
Recipient-ID-Asymmetric:
 ME0xCzAJBgNVBAYTAlVTMSAwHgYDVQQKExdSU0EgRGF0YSBTZWN1cml0eSwgSW5j
 LjEcMBoGA1UECxMTUGVyc29uYSBDZXJ0aWZpY2F0ZQ==,12
```

This field identifies a recipient, and may occur multiple times. The first parameter is an encoding of the name of the issuer of the recipient's certificate, and the second parameter is the serial number of the recipient's certificate. Thus, the recipient is not identified directly. If you decode this particular example, you will see that it says that this recipient is the owner of the 12th certificate issued by RSA Data Security, Inc.

```
Key-Info: RSA,
 UCoYCx7e3nap6HvKN3w5dVs6Nv4Vzw7kwvxE6SRq4c/fr0SL4hJGCZLKTerhb5Ly
 KvUrRTm/9MAmWJNhmT+Hqi925V66QVrDmzazDSMfESM81ovc5APWr2Eb7xNrOEM1
```

Key-Info describes the message key as encrypted under the public key of the most recently-named recipient.

```
Recipient-ID-Asymmetric:
 ME0xCzAJBgNVBAYTAlVTMSAwHgYDVQQKExdSU0EgRGF0YSBTZWN1cml0eSwgSW5j
 LjEcMBoGA1UECxMTUGVyc29uYSBDZXJ0aWZpY2F0ZQ==,16
Key-Info: RSA,
 LookV1eGyPwZJ4sz2Eyf1ak3re3Sti2JeSIIaost1SeW93L3eqcXCAqGz7GBBJfN
 hSziXJDIbNEGGXdm9Zuoc0E=
```

In this example, there are two recipients; hence, there are two occurrences of the recipient identifier & message key fields. Note that in many cases, the first parameter of Recipient-ID-Asymmetric will be identical from one recipient to the next, since often several recipients will have obtained their certificates from the same issuer.

A single blank line separates the headers from the encrypted message. The encrypted message is printably encoded and written out in lines of 64 ASCII characters each (except the last line).

```
vJZOOU8izhi44YZgbGy2U2/oPe+RluWAo6SmPBgVjtgQ+xeZA84uL0Pnljj4moL/
IrzUDgpnzsBqnWcAW2YD7xa7FbJuTC8/cOtgSDLBtmPfc1NhL0JY5eY8Ts7fGSt0
gG0hlfA4deo=
-----END PRIVACY-ENHANCED MESSAGE-----
```

All RIPEM messages end with this line.

Certificates

A certificate is a "document" that states a user, his/her public key component, and validity information. Certificates are printably-encoded. Specifically, a certificate contains the following items. Items of special interest, and most likely to vary from one certificate to another, are marked with a *.

- A version number that applies to the format of the certificate; currently, this is always zero.
- * A serial number. This serial number is unique amoungst all the certificates issued by a given certifying authority.
- The identifier of the algorithm used to sign the certificate. This currently is always the same, and specifies the RSA algorithm.
- * The multi-part name of the issuer of the certificate. There can be many different issuers, but in practise the number of different issuers is likely to be small for the near future.
- The date range during which the certificate is valid. Typically certificates are valid for two years.
- * The multi-part name of the person or entity to whom the certificate was issued. This typically contains not only the proper name of the issuee (e.g., "John Smith"), but the domain with which the issuee is associated (e.g., the issuee's company name ("Acme Widgets") and country ("US")).
- * The public key of the issuee of the certificate. This, obviously, is the whole point of the certificate.
- * The signature of all of the above information in the certificate, done by the issuer with its private key. If you know the issuer's public key, you can verify this signature.

RIPEM-Mode Messages

```
-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 2001,ENCRYPTED
DEK-Info: DES-CBC,194E5E0350762C82
Originator-Name: mrr@scss3.cl.msu.edu
Originator-Key-Asymmetric:
 MFkwCgYEVQgBAQICAgYDSwAwSAJBMpWXPx/qTRUUKhwuGmyUFeIE80bhqF5jhYHX
 j5A7IZgAeHQGuqmPMqbC6gxZl32xCJ488Mc/MHgRxkZ02cBXKzMCAwEAAQ==
Key-Info: RSA,
 IVFGLgKdlQ9pF+qtZpqtJtdxCOJU3ie1SaiVohlmj5zOjs5dl7HZ0UOywTsrR8FN
 /2jrVT3zg1pphJyE+8M9OJY=
MIC-Info: RSA-MD5,RSA,
 hkoroUoBWqFb5HZDcL3M/DhitmLVX+NyhVobd2Eyde5yZEoLbx3f+TLEahJPkrwM
 i9PKBur+9O7H+EmLmrqzRCbPFxL2zHKt
Recipient-Name: test
Key-Info: RSA,
 Atleg3hO2yJfjdEZfGW9FVZcP9CcrEPus5WIzTfqcQzQSgTyldyV5XPMs/87J6xE
 MSaytHpMaThNxZuOnc+EaBs=
Recipient-Name: raylau@mit.edu
Key-Info: RSA,
 RmaSSj2jz1ZU0j9RWFpSTOp01d1iqB2CsPIBH1vaObjC+r2a4U7sOnyfouZMe2+Q
 LVIgy6Vzz862e/K0LwKXbyZaaqrE/swAR6QQZqiTLU53/rPLIJGCRTuCPKYCyTAw

UeluB7ffHqprsJ1cIrD1uJlBmqk90kyML/LEHnyGJys=
-----END PRIVACY-ENHANCED MESSAGE-----
```

RIPEM Public Key Database (aka Directory)

```
User: Raymond Lau.Persona Certificate.RSA Data Security  Inc.
SubjectInfo: CN=Raymond Lau, OU=Persona Certificate, O=RSA Data Security,
Inc., C=US
IssuerInfo: OU=Persona Certificate, O=RSA Data Security, Inc., C=US
SerialNumberInfo: 0x12
CertificateInfo:
 MIIBxTCCAWECARIwDQYJKoZIhvcNAQECBQAwTTELMAkGA1UEBhMCVVMxIDAeBgNV
 BAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMRwwGgYDVQQLExNQZXJzb25hIENl
 cnRpZmljYXRlMB4XDTkzMDQxMjIyNTI1N1oXDTk1MDQxMjA1MDAwMFowYzELMAkG
 A1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMRwwGgYD
 VQQLExNQZXJzb25hIENlcnRpZmljYXRlMRQwEgYDVQQDEwtSYXltb25kIExhdTB5
 MAoGBFUIAQECAgMAA2sAMGgCYQC4Lq5eHwr4u4bY7VggmpOwmyqhq9nMVR7VuaUy
 4MOTPLPHi/dZM5E2gdODG1uV2YoGDNNTuVFRO4osQwxTOWMt9oEththrXOYI6oZ8
 lzyYfmgLVL15S7HCV/GYJdlPuO0CAwEAATANBgkqhkiG9w0BAQIFAANPAAUVNpom
 zLBp6r72gqG6bBU1eFbv9bNKk4WSQCXYRbulGmhyLCXItASYloprlBxKHm8EP178
 P8z1rlbRNAoWw2G5q2550I6UUiJ5OOkVwB==

User: Persona Certificate.RSA Data Security  Inc.
SubjectInfo: OU=Persona Certificate, O=RSA Data Security, Inc., C=US
IssuerInfo: OU=Low Assurance Certification Authority, O=RSA Data Security,
Inc., C=US
SerialNumberInfo: 0x5E000003
CertificateInfo:
 MIIBxjCCAVACBF4AAAMwDQYJKoZIhvcNAQECBQAwXzELMAkGA1UEBhMCVVMxIDAe
 BgNVBAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMS4wLAYDVQQLEyVMb3cgQXNz
 dXJhbmNlIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTkyMTIyMzA4MDAwMFoX
 DTk0MDEwMTA3NTk1OVowTTELMAkGA1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRh
 IFNlY3VyaXR5LCBJbmMuMRwwGgYDVQQLExNQZXJzb25hIENlcnRpZmljYXRlMGkw
 DQYJKoZIhvcNAQEBBQADWAAwVQJOBqoIUA2vV4v9swHWBKiVSHGIZSzdRaSPbV0N
 Zus2d/T2FyvFIaI9BLO5Fkb/IQtOL6pDisJ3Vm81bb6B0Dpj/JzpJLgYvgEL4BaE
 XIDlAgMBAAEwDQYJKoZIhvcNAQECBQADYQCPF1HZAPzWWKSyspFjbUGkmQAWGLtz
 3Zvl1nn3EztPPVtR6GirTpFRa07ov7isHWEdZxGKIwbmFPJuh8pn8tTrSyYfWfD6
 /CHEa04fhZ4jVoAmKmjdgbRTqfraABsBAC9=
Status: Valid by Declaration

User: Mark Riordan.Persona Certificate.RSA Data Security  Inc.
```

SubjectInfo: CN=Mark Riordan, OU=Persona Certificate, O=RSA Data Security, Inc., C=US
IssuerInfo: OU=Persona Certificate, O=RSA Data Security, Inc., C=US
SerialNumberInfo: 0x16
CertificateInfo:

MIIBpjCCAUICARYwDQYJKoZIhvcNAQECBQAwTTELMAkGA1UEBhMCVVMxIDAeBgNV
BAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMRwwGgYDVQQLExNQZXJzb25hIENl
cnRpZmljYXRlMB4XDTkzMDQxOTIwMDI1MFoXDTk1MDQxOTAwMDAwMFowZDELMAkG
A1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMRwwGgYD
VQQLExNQZXJzb25hIENlcnRpZmljYXRlMRUwEwYDVQQDEwxNYXJrIFJpb3JkYW4w
WTAKBgRVCAEBAgICBgNLADBIAkEylZc/H+pNFRQqHC4abJQV4gTzRuGoXmOFgdeP
kDshmAB4dAa6qY8ypsLqDFmXfbEInjzwxz8weBHGRnTZwFcrMwIDAQABMA0GCSqG
SIb3DQEBAgUAA08ABMavdfXztriNQZwk8Ma/YbMOd81sg/bASPXKi2FhmDn2WhdZ
967PW+ZPYkCDn0JdUikP/41xvKuHhOPDNROvN+Sltgf0aFenF2m8/voX

Status: Valid by Declaration

User: test22
PublicKeyInfo:

MFkwCgYEVQgBAQICAgQDSwAwSAJBCcVXx4EuHCsiJgidWtNPyWyTuA5CiTqcKWT8
IujdiMqcSh/iRVO8+nugWDTNwG3LaERzfNe5wLznNpyNSKBwoQcCAwEAAQ==

MD5OfPublicKey: E50F516A4626002DF9B877A8D265BBF8