Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 30, 2012

S. Josefsson
SJD AB

January 27, 2012

Text Encodings of Some Security Related Structures
draft-josefsson-pkix-textual-00

Abstract

This document describe and discuss the text encodings of Public-Key Infrastructure using X.509 (PKIX) Certificates, PKIX Certificate Revocation Lists (CRLs), PKCS #10 Certificate Request Syntax, PKCS #7 structures, and Attribute Certificates. The text encodings are well-known, implemented by several applications and libraries, and is widely deployed. This document is intended to articulate the de-facto rules that existing implementations operate by, and to give recommendations that will promote interoperability going forward.

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

Several security-related standards used on the Internet define data formats that are normally encoded using Distinguished Encoding Rules (DER) [CCITT.X690.2002], which is a binary data format. This document is about text encodings of some of these formats. In particular, we describe text encodings for the following formats.

1. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [RFC5280], for both Certificates and Certificate Revocation Lists (CRLs).
2. PKCS #10: Certification Request Syntax [RFC2986].
3. PKCS #7: Cryptographic Message Syntax [RFC2315].
4. An Internet Attribute Certificate Profile for Authorization [RFC5755].

One motivation for a text encoding is that a binary data format has the disadvantage that it cannot be interchanged in textual transports, such as e-mail or text documents. One advantage with text encodings is that they are easy to modify without special-purpose tools; for example, using a text editor you may concatenate several certificates to form a certificate chain.

The exact history of the text encodings are unknown to the author of this document, however the tradition within the RFC series can be traced back to PEM [RFC1421] and OpenPGP [RFC2015]. These text encodings are sometimes referred to as "PEM encodings". Peter Gutmann's X.509 Style Guide [X509SG] contains a section "base64 Encoding" that describe the formats and contains suggestions similar to what is in this document.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. General Considerations

The structure of a text encoding is such that they begin with a line starting with "-----BEGIN" and end with a line starting with "-----END". Between these markers are Base64 [RFC4648] encoded data. Data before the "-----BEGIN" and after the "-----END" marker are permitted and MUST NOT cause parsers to malfunction. Further, parsers MUST ignore whitespace and other non-alphabetic characters and MUST handle different newline conventions.

The type of data encoded is labeled depending on the type label in

the "-----BEGIN" line. For example, the line may be "-----BEGIN CERTIFICATE-----" to indicate that the content is a PKIX Certificate (see further below). Generators MUST put the same label on the "-----END" line as the corresponding "-----BEGIN" line. Parses MAY disregard the label on the "-----END" lines instead of signalling an error if there is a label mismatch.

The label type is not a guarantee that the encoded data follows the implied syntax. Parsers MUST handle non-conforming data gracefully.

Files MAY contain multiple instances of the text encoded representation. This is used, for example, when a file contains several certificates. Whether the instances are ordered or unordered depends on the context.

Generators MUST wrap the base64 encoded lines so that each line consists of exactly 64 characters except for the final line which will encode as much data is left (within the 64 character line boundary). Parser MAY handle other line sizes.

3. Text Encoding of PKIX Certificate

PKIX Certificates are encoded using the "CERTIFICATE" label. The encoded data MUST be a DER encoded ASN.1 "Certificate" structure as described in section 4 of [RFC5280].

```
-----BEGIN CERTIFICATE-----
MIICLDCCAdKgAwIBAgIBADAKBggqhkjOPQQDAjB9MQswCQYDVQQGEwJCRTEPMA0G
A1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2VydGlmaWNhdGUgYXV0aG9y
aXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdudVRMUyBjZXJ0aWZpY2F0
ZSBhdXRob3JpdHkwHhcNMTEwNTIzMjAzODIxWhcNMTIxMjIyMDc0MTUxWjB9MQsw
CQYDVQQGEwJCRTEPMA0GA1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2Vy
dGlmaWNhdGUgYXV0aG9yaXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdu
dVRMUyBjZXJ0aWZpY2F0ZSBhdXRob3JpdHkwWTATBgcqhkjOPQIBBggqhkjOPQMB
BwNCAARS2I0jiuNn14Y2sSALCX3IybqiIJUvxUpj+oNfzngvj/Niyv2394BWnW4X
uQ4RTEiywK87WRcWMGgJB5kX/t2no0MwQTAPBgNVHRMBAf8EBTADAQH/MA8GA1Ud
DwEB/wQFAwMHBgAwHQYDVR0OBBYEFPC0gf6YEr+1KLlkQAPLzB9mTigDMAoGCCqG
SM49BAMCA0gAMEUCIDGuwD1KPyG+hRf88MeyMQcqOFZD0TbVleF+UsAGQ4enAiEA
l4wOuDwKQa+upc8GftXE2C//4mKANBC6It01gUaTIpo=
-----END CERTIFICATE-----
```

Figure 1: Certificate Example

Historically the label "X509 CERTIFICATE" and also, less common, "X.509 CERTIFICATE" have been used. Generators conforming to this document MUST generate "CERTIFICATE" labels and MUST NOT generate "X509 CERTIFICATE" or "X.509 CERTIFICATE" labels. Parsers are NOT

RECOMMENDED to treat "X509 CERTIFICATE" or "X.509 CERTIFICATE" as equivalent to "CERTIFICATE", but a valid exception may be for backwards compatibility (potentially together with a warning).

4. Text Encoding of PKIX CRLs

PKIX CRLs are encoded using the "X509 CRL" label. The encoded data MUST be a DER encoded ASN.1 "CertificateList" structure as described in section 5 of [RFC5280].

```
-----BEGIN X509 CRL-----
MIIB9DCCAV8CAQEwCwYJKoZIhvcNAQEFMIIBCDEXMBUGA1UEChMOVmVyaVNpZ24s
IEluYy4xHzAdBgNVBAsTFlZlcmlTaWduIFRydXN0IE5ldHdvcmsxRjBEBgNVBAsT
PXd3dy52ZXJpc2lnbi5jb20vcmVwb3NpdG9yeS9SUEEgSW5jb3JwLiBieSBSZWYu
LExJQUIuTFREKGMpOTgxHjAcBgNVBAsTFVBlcnNvbmEgTm90IFZhbGlkYXRlZDEm
MCQGA1UECxMdRGlnaXRhbCBJRCBDbGFzcyAxIC0gTmV0c2NhcGUxGDAWBgNVBAMU
D1NpbW9uIEpvc2Vmc3NvbjEiMCAGCSqGSIb3DQEJARYTc2ltb25Aam9zZWZzc29u
Lm9yZxcNMDYxMjI3MDgwMjM0WhcNMDcwMjA3MDgwMjM1WjAjMCECEC4QNwPfRoWd
elUNpllhhTgXDTA2MTIyNzA4MDIzNFowCwYJKoZIhvcNAQEFA4GBAD0zX+J2hkcc
Nbrq1Dn5IKL8nXLgPGcHv1I/le1MNo9t1ohGQxB5HnFUkRPAY82fR6Epor4aHgVy
b+5y+neKN9Kn2mPF4iiun+a4o26CjJ0pArojCL1p8T0yyi9Xxvyc/ezaZ98HiIyP
c3DGMNR+oUmSjKZ0jIhAYmeLxaPHfQwR
-----END X509 CRL-----
```

Figure 2: CRL Example

Historically the label "CRL" have been used, but today it is not common and several popular tools do not understand the label. Generators conforming to this document MUST generate "X509 CRL" labels and MUST NOT generate "CRL" labels. Parsers are NOT RECOMMENDED to treat "CRL" as equivalent to "X509 CRL".

5. Text Encoding of PKCS #10 Certification Request Syntax

PKCS #10 Certification Requests are encoded using the "CERTIFICATE REQUEST" label. The encoded data MUST be a DER encoded ASN.1 "CertificationRequest" structure as described in [RFC2986].

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWDCCAQcCAQAwTjELMAkGA1UEBhMCU0UxJzAlBgNVBAoTHlNpbW9uIEpvc2Vm
c3NvbiBEYXRha29uc3VsdCBBQjEWMBQGA1UEAxMNam9zZWZzc29uLm9yZzBOMBAG
ByqGSM49AgEGBSuBBAAhAzoABLLPSkuXY0l66MbxVJ3Mot5FCFuqQfn6dTs+9/CM
EOlSwVej77tj56kj9R/j9Q+LfysX8FO9I5p3oGIwYAYJKoZIhvcNAQkOMVMwUTAY
BgNVHREEETAPgg1qb3NlZnNzb24ub3JnMAwGA1UdEwEB/wQCMAAwDwYDVR0PAQH/
BAUDAwegADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDATAKBggqhkjOPQQDAgM/ADA8
AhxBvfhxPFfbBbsE1NoFmCUczOFApEuQVUw3ZP69AhwWXk3dgSUsKnuwL5g/ftAY
dEQc8B8jAcnuOrfU
-----END CERTIFICATE REQUEST-----
```

Figure 3: PKCS #10 Example

The label "NEW CERTIFICATE REQUEST" is also in wide use. Generators conforming to this document MUST generate "CERTIFICATE REQUEST" labels. Parsers MAY treat "NEW CERTIFICATE REQUEST" as equivalent to "CERTIFICATE REQUEST".

6. Text Encoding of PKCS #7 Cryptographic Message Syntax

PKCS #7 Cryptographic Message Syntax structures are encoded using the "PKCS7" label. The encoded data MUST be a DER encoded ASN.1 "ContentInfo" structure as described in [RFC2315].

```
-----BEGIN PKCS7-----
MIHjBgsqhkiG9w0BCRABF6CB0zCB0AIBADFho18CAQCgGwYJKoZIhvcNAQUMMA4E
CLfrI6dr0gUWAgITiDAjBgsqhkiG9w0BCRADCTAUBggqhkiG9w0DBwQIZpECRWtz
u5kEGDCjerXY8odQ7EEEromZJvAurk/j81IrozBSBgkqhkiG9w0BBwEwMwYLKoZI
hvcNAQkQAw8wJDAUBggqhkiG9w0DBwQI0tCBcU09nxEwDAYIKwYBBQUIAQIFAIAQ
OsYGYUFdAH0RNc1p4VbKEAQUM2Xo8PMHBoYdqEcsbTodlCFAZH4=
-----END PKCS7-----
```

Figure 4: PKCS #7 Example

The label "CERTIFICATE CHAIN" has been in use to denote a degenerative PKCS #7 structure that contains only a list of certificates. Several modern tools do not support this label. Generators MUST NOT generate the "CERTIFICATE CHAIN" label. Parsers are NOT RECOMMENDED to treat "CERTIFICATE CHAIN" as equivalent to "PKCS7".

7. Text Encoding of Attribute Certificates

Attribute certificates are encoded using the "ATTRIBUTE CERTIFICATES" label. The encoded data MUST be a DER encoded ASN.1 "AttributeCertificate" structure as described in [RFC5755].

```
-----BEGIN ATTRIBUTE CERTIFICATE-----
MIICKzCCAZQCAQEwgZeggZQwgYmkgYYwgYMxCzAJBgNVBAYTAlVTMREwDwYDVQQI
DAhOZXcgWW9yazEUMBIGA1UEBwwLU3RvbnkgQnJvb2sxDzANBgNVBAoMBkNTRTU5
MjE6MDgGA1UEAwwxU2NvdHQgU3RhbGxlci9lbWFpbEFkZHJlc3M9c3N0YWxsZXJA
aWMuc3VueXNiLmVkdQIGARWrgUUSoIGMMIGJpIGGMIGDMQswCQYDVQQGEwJVUzER
MA8GA1UECAwITmV3IFlvcmsxFDASBgNVBAcMC1N0b255IEJyb29rMQ8wDQYDVQQK
DAZDU0U1OTIxOjA4BgNVBAMMMVNjb3R0IFN0YWxsZXIvZW1haWxBZGRyZXNzPXNz
dGFsbGVyQGljLnN1bnlzYi5lZHUwDQYJKoZIhvcNAQEFBQACBgEVq4FFSjAiGA8z
OTA3MDIwMTA1MDAwMFoYDzM5MTEwMTMxMDUwMDAwWjArMCkGA1UYSDEiMCCGHmh0
dHA6Ly9pZGVyYXNobi5vcmcvaW5kZXguaHRtbDANBgkqhkiG9w0BAQUFAAOBgQAV
M9axFPXXozEFcer06bj9MCBBCQLtAM7ZXcZjcxyva7xCBDmtZXPYUluHf5OcWPJz
5XPus/xS9wBgtlM3fldIKNyNO8RsMp6Ocx+PGlICc7zpZiGmCYLl64lAEGPO/bsw
Smluak1aZIttePeTAHeJJs8izNJ5aR3Wcd3A5gLztQ==
-----END ATTRIBUTE CERTIFICATE-----
```

Figure 5: Attribute Certificate Example

8. Non-comforming Examples

This section contains examples for the non-recommended label variants described earlier in this document. As discussed earlier, supporting these are not required and sometimes discouraged. Still, they can be useful for interoperability testing and for easy reference.

```
-----BEGIN X509 CERTIFICATE-----
MIICLDCCAdKgAwIBAgIBADAKBggqhkjOPQQDAjB9MQswCQYDVQQGEwJCRTEPMA0G
A1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2VydGlmaWNhdGUgYXV0aG9y
aXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdudVRMUyBjZXJ0aWZpY2F0
ZSBhdXRob3JpdHkwHhcNMTEwNTIzMjAzODIxWhcNMTIxMjIyMDc0MTUxWjB9MQsw
CQYDVQQGEwJCRTEPMA0GA1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2Vy
dGlmaWNhdGUgYXV0aG9yaXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdu
dVRMUyBjZXJ0aWZpY2F0ZSBhdXRob3JpdHkwWTATBgcqhkjOPQIBBggqhkjOPQMB
BwNCAARS2I0jiuNn14Y2sSALCX3IybqiIJUvxUpj+oNfzngvj/Niyv2394BWnW4X
uQ4RTEiywK87WRcWMGgJB5kX/t2no0MwQTAPBgNVHRMBAf8EBTADAQH/MA8GA1Ud
DwEB/wQFAwMHBgAwHQYDVR0OBBYEFPC0gf6YEr+1KLlkQAPLzB9mTigDMAoGCCqG
SM49BAMCA0gAMEUCIDGuwD1KPyG+hRf88MeyMQcqOFZD0TbVleF+UsAGQ4enAiEA
l4wOuDwKQa+upc8GftXE2C//4mKANBC6It01gUaTIpo=
-----END X509 CERTIFICATE-----
```

Figure 6: Non-standard 'X509' Certificate Example

```
-----BEGIN X.509 CERTIFICATE-----
MIICLDCCAdKgAwIBAgIBADAKBggqhkjOPQQDAjB9MQswCQYDVQQGEwJCRTEPMA0G
A1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2VydGlmaWNhdGUgYXV0aG9y
aXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdudVRMUyBjZXJ0aWZpY2F0
ZSBhdXRob3JpdHkwHhcNMTEwNTIzMjAzODIxWhcNMTIxMjIyMDc0MTUxWjB9MQsw
CQYDVQQGEwJCRTEPMA0GA1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2Vy
dGlmaWNhdGUgYXV0aG9yaXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdu
dVRMUyBjZXJ0aWZpY2F0ZSBhdXRob3JpdHkwWTATBgcqhkjOPQIBBggqhkjOPQMB
BwNCAARS2I0jiuNn14Y2sSALCX3IybqiIJUvxUpj+oNfzngvj/Niyv2394BWnW4X
uQ4RTEiywK87WRcWMGgJB5kX/t2no0MwQTAPBgNVHRMBAf8EBTADAQH/MA8GA1Ud
DwEB/wQFAwMHBgAwHQYDVR0OBBYEFPC0gf6YEr+1KLlkQAPLzB9mTigDMAoGCCqG
SM49BAMCA0gAMEUCIDGuwD1KPyG+hRf88MeyMQcqOFZD0TbVleF+UsAGQ4enAiEA
l4wOuDwKQa+upc8GftXE2C//4mKANBC6It01gUaTIpo=
-----END X.509 CERTIFICATE-----
```

Figure 7: Non-standard 'X.509' Certificate Example

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBWDCCAQcCAQAwTjELMAkGA1UEBhMCU0UxJzAlBgNVBAoTHlNpbW9uIEpvc2Vm
c3NvbiBEYXRha29uc3VsdCBBQjEWMBQGA1UEAxMNam9zZWZzc29uLm9yZzBOMBAG
ByqGSM49AgEGBSuBBAAhAzoABLLPSkuXY0l66MbxVJ3Mot5FCFuqQfn6dTs+9/CM
EOlSwVej77tj56kj9R/j9Q+LfysX8FO9I5p3oGIwYAYJKoZIhvcNAQkOMVMwUTAY
BgNVHREEETAPgg1qb3NlZnNzb24ub3JnMAwGA1UdEwEB/wQCMAAwDwYDVR0PAQH/
BAUDAwegADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDATAKBggqhkjOPQQDAgM/ADA8
AhxBvfhxPFfbBbsE1NoFmCUczOFApEuQVUw3ZP69AhwWXk3dgSUsKnuwL5g/ftAY
dEQc8B8jAcnuOrfU
-----END NEW CERTIFICATE REQUEST-----
```

Figure 8: Non-standard 'NEW' PKCS #10 Example

```
-----BEGIN CERTIFICATE CHAIN-----
MIHjBgsqhkiG9w0BCRABF6CB0zCB0AIBADFho18CAQCgGwYJKoZIhvcNAQUMMA4E
CLfrI6dr0gUWAgITiDAjBgsqhkiG9w0BCRADCTAUBggqhkiG9w0DBwQIZpECRWtz
u5kEGDCjerXY8odQ7EEEromZJvAurk/j81IrozBSBgkqhkiG9w0BBwEwMwYLKoZI
hvcNAQkQAw8wJDAUBggqhkiG9w0DBwQI0tCBcU09nxEwDAYIKwYBBQUIAQIFAIAQ
OsYGYUFdAH0RNc1p4VbKEAQUM2Xo8PMHBoYdqEcsbTodlCFAZH4=
-----END CERTIFICATE CHAIN-----
```

Figure 9: Non-standard 'CERTIFICATE CHAIN' Example

9. Security Considerations

Data in this format is often originating from untrusted sources, thus parsers must be prepared to handle unexpected data without causing security vulnerabilities.

By having more than one canonical encoding of the same data, an ambiguity is introduced. The first one is introduced by permitting the text encoded representation instead of the binary DER encoding, but further ambiguities arise when multiple labels are treated as similar. Even further, variations of whitespace and non-base64 alphabetic characters can further create ambiguities. Implementations that rely on canonical representation or the ability to fingerprint a particular data format will need to take this into account. Data encoding ambiguities also create opportunities for side channels.

10. IANA Considerations

This document implies no IANA Considerations.

11. Acknowledgements

Peter Gutmann suggested to document labels for Attribute Certificates and PKCS #7 messages, and to add examples for the non-standard variants.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, March 1998.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, November 2000.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5755] Farrell, S., Housley, R., and S. Turner, "An Internet Attribute Certificate Profile for Authorization",

RFC 5755, January 2010.

[CCITT.X690.2002]
International International Telephone and Telegraph Consultative Committee, "ASN.1 encoding rules: Specification of basic encoding Rules (BER), Canonical encoding rules (CER) and Distinguished encoding rules (DER)", CCITT Recommendation X.690, July 2002.

12.2. Informative References

[RFC1421] Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", RFC 1421, February 1993.

[RFC2015] Elkins, M., "MIME Security with Pretty Good Privacy (PGP)", RFC 2015, October 1996.

[X509SG] Gutmann, P., "X.509 Style Guide", WWW http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt.

Author's Address

Simon Josefsson
SJD AB
Johan Olof Wallins Vaeg 13
Solna 171 64
SE

Email: simon@josefsson.org
URI: http://josefsson.org/