

Chunk Registration Request for Enabling the PNG Standard to Support Digital Signatures

Commented Example

Thomas Kopp / Dialogika GmbH

This document outlines a detailed example for the **dSIG** chunk request (version 1.3).

The optional yet important PNG digital signature feature can be applied to various use cases, e.g. for cleaning web pages that may contain dangerous PNGs hiding malicious scripts attached by intruders.

The example has been elaborated and commented by **Martin BoBlet** who also provided a proof of concept for signing and verifying PNG images.

The following PNG image has been used for attaching a digital signature.



```
89504E470D0A1A0A # PNG 8-byte signature (not included in the message digest)

0000000D # IHDR: length 13

49484452 # IHDR

000001A40000012C0806000000 # IHDR data

8CAFC780 # IHDR CRC

00000021 # dSIG: length 33 (introductory dSIG chunk)

64534947 # dSIG

301F
020101
310B
3009
06052B0E03021A
0500
300B
06092A864886F70D010701
3100 # dSIG data

<<
```

The data is the DER encoding of the following ASN.1 structure:

```
SEQUENCE {
    INTEGER 1
```

```

SET {
    SEQUENCE {
        OBJECT IDENTIFIER 1.3.14.3.2.26
        NULL
    }
}

SEQUENCE {
    OBJECT IDENTIFIER 1.2.840.113549.1.7.1
}

SET {
}
}

```

The structure represents a signed data instance specified in RFC 3852:

```

SignedData ::= SEQUENCE {
    version CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates [0] IMPLICIT CertificateSet OPTIONAL,
    crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,
    signerInfos SignerInfos
}

```

The following particularities can be observed:

The version is 1.

The digest algorithms structure contains the SHA-1 identifier.

The encapsulated content is empty and specified by the id data object identifier.

Certificates and CRLs are omitted.

The structure contains an empty set of signer infos.

The introductory dSIG chunk serves for the sole purpose to inform a verifier about the digest algorithms used in order to support streamed processing.

>>

FF5690A9 # dSIG CRC

```

00000001 # sRGB: length 1

73524742 # sRGB

00 # sRGB data

AECE1CE9 # sRGB CRC

00000006 # bKGD: length 6

624B4744 # bKGD

00F600C2000E # bKGD data

4BA471AB # bKGD CRC

00000009 # pHYs: length 9

70485973 # pHYs

00000B1300000B1301 # pHYs data

009A9C18 # pHYs CRC

00000007 # tIME: length 7

74494D45 # tIME

07D8040F0A0110 # tIME data

96612687 # tIME CRC

00000019 # tEXt: length 25

74455874 # tEXt

436F6D6D656E74004372656174656420776974682047494D50 # tEXt data (origin: GIMP)

57810E17 # tEXt CRC

00002000 # IDAT: length 8192

49444154 # IDAT:

[Omitted 10 IDAT chunks of 8192 bytes each, followed by a final one of 3172
bytes.]

D2B26128 # last IDAT CRC

00000654 # dSIG: length 1620

64534947 # dSIG

30820650
020101
3100
300B
06092A864886F70D010701
A0820547
30820543
3082042B

```

A003
020102
02020A4F

300D
06092A864886F70D010105
0500

3045
310B
3009
0603550406
13024C55

3115
3013
060355040A
130C4C7578547275737420732E61

311F
301D
0603550403
13164C75785472757374204E6F726D616C69736564204341

301E
170D3037303532313133303031345A
170D3130303532313133303031345A

30820100
310B
3009
0603550406
13024445

3110
300E
0603550407
13074765726D616E79

3117
3015
060355040A
130E4469616C6F67696B6120476D6248

3115
3013
060355040B
130C485242204E722E2037333437

311D
301B
0603550403
13144D617274696E20506574657220426F73736C6574

3110
300E
0603550404
1307426F73736C6574

3115
3013
060355042A
130C4D617274696E205065746572
311D
301B
0603550405

13143130313030333832343830303030323130393830

312A

3028

06092A864886F70D010901

161B6D617274696E2E626F73736C6574406469616C6F67696B612E6465

311C

301A

060355040C

131350726F66657373696F6E616C20506572736F6E

30819F

300D

06092A864886F70D010101

0500

03818D

0030818902818100A5318FD0FBF26C6A2377B4488D5FCF52282B2B25AAC6A0003FD3BC8B

0377804F8DEC8394D54469DA6417F0E274852FAB422B0A6B2E94FFF9A3F170FB8947FCF2

5E2C5E1FDB74EC2F8C9C862C4F52BC33CA34F4825512BC6D32798D33D12950A6F678EA40

46F007317104C5661AB838E0939AD9D84647E377DFDDC6B5936A9BF50203010001

A3820202

308201FE

300C

0603551D13

0101FF

04023000

3060

06082B06010505070101

04543052302306082B060105050730018617687474703A2F2F6F6373702E6C7578747275

73742E6C75302B06082B06010505073002861F687474703A2F2F63612E6C757874727573

742E6C752F4C544E43412E637274

3082010A

0603551D20

048201013081FE3008060604008F7A01023081F106072B812B010201013081E53081B706

082B060105050702023081AA1A81A74C75785472757374204E6F726D616C697365642043

65727469666963617465206F6E20535343442E2055736167653A20456C656374726F6E69

63205369676E617475726520284F494420312E332E3137312E312E322E312E3129204175

7468656E7469636174696F6E2020616E6420456E6372797074696F6E20284F4944312E33

2E3137312E312E322E312E32292E204B65792047656E65726174696F6E20627920435350

2E20302906082B06010505070201161D687474703A2F2F7265706F7369746F72792E6C75

7874727573742E6C75

300B

0603551D0F

0404030204B0

301F

0603551D23

041830168014CEFE469D632F89FDF2381625D8F16CDE47F8CEC1

3031

0603551D1F

042A30283026A024A0228620687474703A2F2F63726C2E6C757874727573742E6C752F4C

544E43412E63726C

301D

0603551D0E

041604149B93CC4AA2F18692880D41AB02D3C6BBDD362452

300D

06092A864886F70D010105

0500

03820101
00B76BE507F770E0D3018178BFA2AD55B4FF455FDB58258C7B65305E2220D8E8B723A8AA
F7F57A9369387938F22A8AEC22EA9946F2E5F1C5DD60F447A98407F6508457A42EE203D3
68DEF26520E52B8BE52475630ED605E187B78494DF8A92AC14527A5390B2E05481E58726
9B3C02DB308179A9947663CC7BBECF1FCC8FCEE95DC76A88C9FB082F1F1627E8DB5C0CC4
5411FD08D79F9EC7D949D5A94096B352F84719533F1442DAEE9BC55386C33BC56455852D
087282FC1443D225C763DB1C800EC777D3907C55797199212165FBBA7ADA01B192D1BF3D
45E5A073F80652760AEBF772D81764A7622956F4D1942BD36CBF98EDF8EC096427C098DA
087D4ED232

3181F0
3081ED
020101

304B
3045

310B
3009
0603550406
13024C55

3115
3013
060355040A
130C4C7578547275737420732E61

311F
301D
0603550403
13164C75785472757374204E6F726D616C69736564204341

02020A4F

3009
06052B0E03021A
0500

300D
06092A864886F70D010101
0500

048180
93B2F085AF3806A86EE61094C2168990BD1C7205B4E7469209324A76E3D47B0D8E80A446
D363A2B3850AEA41C5C1D6F2A5E064496E122E5248D060C4FE38B0C7C9AE6DCE54E813C4
09C5324793A7139E162B2ABFE BBB0DC9E0B65E5C802163B1971762C9D60A9CC1CB2AF477
55B91D35A49248ECF1171521CD39043E2062ADEE

dSIG data

<<

The terminating dSIG chunk again is a DER-encoded signed data instance:

SEQUENCE {

INTEGER 1

SET {

}

```

SEQUENCE {
    OBJECT IDENTIFIER 1.2.840.113549.1.7.1
}
[0] {
    SEQUENCE {
        SEQUENCE {
            [0] {
                INTEGER 2
            }
            INTEGER 2639
            SEQUENCE {
                OBJECT IDENTIFIER 1.2.840.113549.1.1.5
                NULL
            }
            SEQUENCE {
                SET {
                    SEQUENCE {
                        OBJECT IDENTIFIER 2.5.4.6
                        PrintableString LU
                    }
                }
                SET {
                    SEQUENCE {
                        OBJECT IDENTIFIER 2.5.4.10
                        PrintableString LuxTrust s.a
                    }
                }
            }
        }
    }
}

```



```

    }
    SET {
        SEQUENCE {
            OBJECT IDENTIFIER 2.5.4.3
            PrintableString LuxTrust Normalised CA
        }
    }
}
SEQUENCE {
    UTCTime Mon May 21 15:00:14 CEST 2007
    UTCTime Fri May 21 15:00:14 CEST 2010
}
SEQUENCE {
    SET {
        SEQUENCE {
            OBJECT IDENTIFIER 2.5.4.6
            PrintableString DE
        }
    }
    SET {
        SEQUENCE {
            OBJECT IDENTIFIER 2.5.4.7
            PrintableString Germany
        }
    }
    SET {

```

```
SEQUENCE {
    OBJECT IDENTIFIER 2.5.4.10
    PrintableString Dialogika GmbH
}
}
SET {
    SEQUENCE {
        OBJECT IDENTIFIER 2.5.4.11
        PrintableString HRB Nr. 7347
    }
}
SET {
    SEQUENCE {
        OBJECT IDENTIFIER 2.5.4.3
        PrintableString Martin Peter Bosslet
    }
}
SET {
    SEQUENCE {
        OBJECT IDENTIFIER 2.5.4.4
        PrintableString Bosslet
    }
}
SET {
    SEQUENCE {
        OBJECT IDENTIFIER 2.5.4.42
```

```

    PrintableString Martin Peter
  }
}
SET {
  SEQUENCE {
    OBJECT IDENTIFIER 2.5.4.5
    PrintableString 10100382480000210980
  }
}
SET {
  SEQUENCE {
    OBJECT IDENTIFIER 1.2.840.113549.1.9.1
    IA5String martin.bosslet@dialogika.de
  }
}
SET {
  SEQUENCE {
    OBJECT IDENTIFIER 2.5.4.12
    PrintableString Professional Person
  }
}
}
SEQUENCE {
  SEQUENCE {
    OBJECT IDENTIFIER 1.2.840.113549.1.1.1
    NULL null
  }
}

```

}

BIT STRING {2, 3, 8, 15, 16, 20, 23, 30, 32, 39, 40, 47, 56, 58, 61, 63, 66, 67, 71, 72, 76, 77, 78, 79, 80, 81, 83, 88, 89, 90, 91, 92, 94, 95, 96, 97, 98, 99, 102, 105, 106, 108, 109, 113, 114, 116, 118, 122, 126, 127, 129, 130, 131, 133, 134, 135, 136, 138, 139, 141, 145, 148, 152, 156, 157, 159, 161, 163, 164, 165, 166, 167, 168, 169, 172, 173, 174, 175, 177, 179, 182, 186, 188, 194, 196, 198, 199, 202, 204, 206, 207, 210, 213, 215, 216, 218, 220, 222, 224, 225, 229, 230, 232, 234, 250, 251, 252, 253, 254, 255, 256, 257, 259, 262, 263, 264, 266, 267, 268, 269, 272, 276, 278, 279, 286, 287, 289, 290, 291, 293, 294, 295, 296, 305, 308, 309, 310, 311, 312, 316, 317, 319, 320, 321, 322, 324, 325, 328, 334, 335, 336, 339, 341, 344, 345, 347, 349, 351, 353, 357, 361, 362, 364, 367, 368, 369, 371, 372, 374, 377, 378, 381, 387, 389, 390, 391, 392, 393, 394, 395, 400, 401, 402, 406, 409, 410, 411, 413, 416, 421, 423, 426, 428, 429, 430, 431, 432, 434, 436, 438, 439, 441, 446, 450, 452, 454, 455, 460, 462, 465, 466, 468, 470, 471, 474, 476, 477, 478, 480, 483, 485, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 503, 504, 506, 510, 511, 512, 513, 514, 515, 519, 521, 522, 523, 528, 529, 530, 531, 532, 534, 535, 536, 540, 543, 545, 549, 550, 551, 552, 553, 554, 555, 556, 557, 560, 561, 562, 563, 566, 569, 571, 572, 573, 574, 578, 580, 581, 585, 587, 588, 589, 590, 595, 596, 597, 598, 599, 600, 601, 603, 604, 606, 607, 609, 610, 611, 613, 616, 617, 618, 620, 621, 626, 628, 629, 630, 631, 632, 636, 637, 640, 643, 644, 645, 648, 653, 654, 658, 660, 661, 665, 668, 669, 670, 671, 673, 675, 678, 680, 682, 683, 684, 685, 690, 691, 694, 695, 696, 697, 700, 702, 706, 707, 709, 712, 713, 714, 715, 717, 720, 726, 729, 731, 733, 735, 739, 742, 744, 746, 747, 748, 749, 753, 754, 756, 757, 759, 762, 763, 766, 769, 770, 771, 772, 775, 776, 780, 781, 783, 786, 787, 790, 791, 792, 793, 795, 799, 802, 804, 807, 809, 811, 816, 818, 821, 822, 824, 825, 826, 827, 829, 830, 833, 834, 835, 836, 840, 841, 842, 844, 846, 849, 857, 861, 862, 864, 865, 866, 867, 877, 878, 879, 882, 883, 887, 889, 890, 891, 895, 901, 904, 905, 909, 911, 913, 914, 917, 918, 923, 924, 926, 928, 930, 931, 932, 938, 939, 940, 944, 945, 946, 952, 955, 958, 959, 960, 963, 964, 966, 968, 969, 971, 972, 975, 976, 977, 979, 980, 985, 989, 990, 993, 997, 998, 999, 1000, 1001, 1002, 1006, 1007, 1009, 1010, 1011, 1013, 1014, 1015, 1016, 1017, 1019, 1020, 1021, 1022, 1023, 1024, 1025, 1027, 1028, 1029, 1031, 1032, 1033, 1037, 1038, 1040, 1042, 1043, 1045, 1047, 1048, 1051, 1054, 1055, 1057, 1058, 1060, 1062, 1064, 1067, 1068, 1070, 1071, 1072, 1073, 1074, 1075, 1077, 1079, 1086, 1094, 1095, 1103, 1119}

}

[3] {

SEQUENCE {

SEQUENCE {

OBJECT IDENTIFIER 2.5.29.19

BOOLEAN true

```

    OCTET STRING 30 00

}

SEQUENCE {

    OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1

    OCTET STRING { 30 52 30 23 06 08 2B 06 01 05 05 07 30 01 86 17
68 74 74 70 3A 2F 2F 6F 63 73 70 2E 6C 75 78 74 72 75 73 74 2E 6C 75 30 2B 06 08
2B 06 01 05 05 07 30 02 86 1F 68 74 74 70 3A 2F 2F 63 61 2E 6C 75 78 74 72 75 73 74
2E 6C 75 2F 4C 54 4E 43 41 2E 63 72 74

    }

SEQUENCE {

    OBJECT IDENTIFIER 2.5.29.32

    OCTET STRING { 30 81 FE 30 08 06 06 04 00 8F 7A 01 02 30 81
F1 06 07 2B 81 2B 01 02 01 01 30 81 E5 30 81 B7 06 08 2B 06 01 05 05 07 02 02 30 81
AA 1A 81 A7 4C 75 78 54 72 75 73 74 20 4E 6F 72 6D 61 6C 69 73 65 64 20 43 65 72
74 69 66 69 63 61 74 65 20 6F 6E 20 53 53 43 44 2E 20 55 73 61 67 65 3A 20 45 6C 65
63 74 72 6F 6E 69 63 20 53 69 67 6E 61 74 75 72 65 20 28 4F 49 44 20 31 2E 33 2E 31
37 31 2E 31 2E 32 2E 31 2E 31 29 20 41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 20
61 6E 64 20 45 6E 63 72 79 70 74 69 6F 6E 20 28 4F 49 44 31 2E 33 2E 31 37 31 2E
31 2E 32 2E 31 2E 32 29 2E 20 4B 65 79 20 47 65 6E 65 72 61 74 69 6F 6E 20 62 79
20 43 53 50 2E 20 30 29 06 08 2B 06 01 05 05 07 02 01 16 1D 68 74 74 70 3A 2F 2F 72
65 70 6F 73 69 74 6F 72 79 2E 6C 75 78 74 72 75 73 74 2E 6C 75

    }

SEQUENCE {

    OBJECT IDENTIFIER 2.5.29.15

    OCTET STRING 03 02 04 B0

    }

SEQUENCE {

    OBJECT IDENTIFIER 2.5.29.35

    OCTET STRING { 30 16 80 14 CE FE 46 9D 63 2F 89 FD F2 38
16 25 D8 F1 6C DE 47 F8 CE C1

    }

}

```

```

SEQUENCE {
    OBJECT IDENTIFIER 2.5.29.31
        OCTET STRING { 30 28 30 26 A0 24 A0 22 86 20 68 74 74 70
3A 2F 2F 63 72 6C 2E 6C 75 78 74 72 75 73 74 2E 6C 75 2F 4C 54 4E 43 41 2E 63 72
6C
        }
    SEQUENCE {
        OBJECT IDENTIFIER 2.5.29.14
            OCTET STRING 04 14 9B 93 CC 4A A2 F1 86 92 88 0D 41 AB
02 D3 C6 BB DD 36 24 52
            }
        }
    }
}

SEQUENCE {
    OBJECT IDENTIFIER 1.2.840.113549.1.1.5
        NULL null
    }

    BIT STRING {0, 2, 3, 5, 6, 7, 9, 10, 12, 14, 15, 16, 17, 18, 21, 23, 29, 30, 31, 32,
33, 34, 35, 37, 38, 39, 41, 42, 43, 48, 49, 50, 56, 57, 59, 62, 63, 71, 72, 79, 81, 82, 83, 84,
88, 90, 91, 92, 93, 94, 95, 96, 98, 102, 104, 106, 108, 109, 111, 113, 115, 117, 119, 120,
122, 123, 125, 128, 129, 130, 131, 132, 133, 134, 135, 137, 141, 143, 145, 147, 148, 149,
150, 151, 152, 153, 155, 156, 158, 159, 161, 163, 164, 170, 173, 175, 176, 180, 181, 185,
186, 187, 188, 190, 191, 193, 194, 197, 199, 202, 203, 209, 211, 212, 213, 214, 218, 222,
226, 232, 233, 235, 236, 240, 241, 242, 244, 248, 250, 251, 253, 254, 255, 258, 262, 263,
264, 266, 268, 272, 274, 276, 278, 280, 281, 282, 283, 285, 286, 287, 288, 289, 290, 291,
293, 295, 297, 298, 299, 300, 302, 304, 307, 310, 311, 313, 314, 316, 319, 322, 323, 324,
329, 330, 331, 332, 335, 338, 339, 340, 344, 345, 346, 347, 350, 354, 356, 358, 360, 364,
366, 368, 369, 370, 372, 373, 378, 382, 384, 385, 386, 388, 390, 392, 395, 396, 399, 401,
405, 406, 408, 409, 410, 411, 414, 416, 417, 418, 421, 423, 424, 425, 426, 427, 431, 432,
433, 437, 439, 440, 441, 443, 444, 445, 447, 449, 450, 456, 457, 458, 459, 461, 465, 469,
470, 471, 472, 474, 476, 479, 480, 485, 493, 494, 495, 496, 497, 498, 499, 501, 502, 505,
507, 512, 517, 521, 523, 525, 526, 527, 528, 530, 533, 538, 540, 541, 542, 544, 545, 546,

```

550, 558, 559, 560, 561, 563, 566, 567, 569, 570, 572, 576, 577, 579, 580, 581, 582, 584, 585, 586, 587, 590, 593, 594, 597, 599, 602, 608, 609, 610, 613, 615, 618, 620, 622, 623, 624, 628, 630, 631, 632, 633, 634, 637, 639, 642, 645, 649, 650, 651, 653, 655, 657, 658, 662, 663, 668, 669, 670, 672, 673, 675, 677, 678, 685, 687, 688, 689, 690, 695, 696, 701, 702, 703, 704, 706, 707, 709, 710, 711, 712, 717, 720, 723, 725, 728, 729, 731, 732, 733, 734, 735, 736, 740, 742, 744, 747, 750, 752, 754, 756, 757, 763, 765, 769, 771, 774, 777, 778, 779, 780, 782, 785, 787, 790, 791, 792, 795, 800, 802, 803, 806, 808, 809, 810, 817, 819, 821, 824, 831, 832, 833, 834, 837, 839, 840, 845, 846, 847, 850, 853, 854, 856, 859, 860, 862, 863, 866, 867, 868, 869, 878, 880, 881, 883, 884, 886, 887, 890, 891, 896, 903, 905, 906, 907, 908, 911, 912, 914, 916, 919, 920, 923, 925, 929, 930, 931, 933, 934, 937, 938, 942, 943, 944, 945, 948, 949, 953, 954, 955, 956, 958, 959, 960, 962, 963, 964, 965, 966, 968, 969, 972, 973, 974, 975, 979, 980, 981, 982, 983, 984, 985, 988, 989, 992, 996, 997, 998, 999, 1000, 1001, 1004, 1005, 1006, 1008, 1009, 1010, 1012, 1015, 1017, 1019, 1020, 1021, 1023, 1024, 1025, 1029, 1030, 1031, 1033, 1034, 1036, 1038, 1040, 1044, 1048, 1049, 1052, 1055, 1056, 1057, 1058, 1059, 1060, 1062, 1063, 1068, 1074, 1076, 1077, 1078, 1079, 1083, 1084, 1085, 1086, 1087, 1091, 1093, 1094, 1098, 1101, 1102, 1103, 1104, 1105, 1106, 1108, 1112, 1113, 1115, 1116, 1118, 1119, 1121, 1123, 1124, 1125, 1132, 1133, 1136, 1137, 1141, 1145, 1147, 1149, 1155, 1159, 1160, 1161, 1162, 1163, 1164, 1165, 1167, 1172, 1176, 1177, 1179, 1181, 1182, 1183, 1184, 1187, 1188, 1189, 1190, 1191, 1192, 1195, 1196, 1197, 1198, 1200, 1201, 1205, 1206, 1207, 1208, 1209, 1211, 1212, 1215, 1217, 1220, 1223, 1224, 1225, 1227, 1229, 1231, 1232, 1234, 1236, 1239, 1241, 1248, 1251, 1253, 1254, 1256, 1258, 1259, 1262, 1263, 1265, 1267, 1270, 1272, 1273, 1274, 1275, 1276, 1281, 1285, 1286, 1287, 1291, 1292, 1295, 1297, 1299, 1302, 1303, 1306, 1307, 1308, 1309, 1310, 1311, 1315, 1317, 1321, 1326, 1328, 1329, 1331, 1332, 1334, 1336, 1337, 1338, 1340, 1341, 1342, 1344, 1347, 1348, 1350, 1351, 1352, 1353, 1357, 1359, 1361, 1363, 1366, 1367, 1368, 1373, 1374, 1376, 1377, 1382, 1383, 1386, 1387, 1388, 1390, 1391, 1392, 1393, 1397, 1399, 1401, 1402, 1405, 1409, 1411, 1413, 1415, 1416, 1421, 1423, 1426, 1428, 1429, 1431, 1436, 1441, 1442, 1443, 1446, 1448, 1454, 1456, 1457, 1458, 1459, 1460, 1461, 1467, 1469, 1473, 1478, 1479, 1480, 1481, 1483, 1486, 1490, 1493, 1495, 1496, 1497, 1501, 1502, 1503, 1505, 1506, 1510, 1511, 1512, 1513, 1515, 1516, 1518, 1519, 1523, 1524, 1525, 1528, 1540, 1541, 1542, 1544, 1545, 1549, 1550, 1551, 1553, 1554, 1555, 1557, 1558, 1559, 1560, 1561, 1563, 1566, 1567, 1568, 1571, 1577, 1578, 1579, 1580, 1581, 1585, 1587, 1589, 1591, 1593, 1594, 1595, 1596, 1599, 1601, 1602, 1603, 1607, 1608, 1611, 1612, 1615, 1618, 1623, 1626, 1631, 1633, 1634, 1637, 1639, 1640, 1641, 1642, 1643, 1644, 1646, 1647, 1648, 1650, 1651, 1652, 1654, 1657, 1658, 1659, 1660, 1662, 1664, 1665, 1667, 1668, 1670, 1679, 1680, 1682, 1683, 1687, 1688, 1691, 1694, 1696, 1697, 1699, 1703, 1704, 1706, 1707, 1708, 1709, 1710, 1711, 1714, 1715, 1716, 1717, 1719, 1721, 1725, 1727, 1728, 1729, 1730, 1733, 1735, 1736, 1738, 1745, 1746, 1747, 1750, 1751, 1752, 1753, 1754, 1755, 1756, 1765, 1766, 1769, 1771, 1774, 1777, 1778, 1779, 1781, 1782, 1788, 1790, 1792, 1793, 1794, 1796, 1798, 1799, 1800, 1801, 1802, 1803, 1805, 1806, 1807, 1809, 1810, 1811, 1814, 1816, 1817, 1819, 1820, 1827, 1829, 1830, 1831, 1833,

1834, 1837, 1840, 1842, 1845, 1846, 1847, 1849, 1850, 1854, 1858, 1860, 1863, 1865, 1867, 1869, 1870, 1872, 1873, 1874, 1875, 1877, 1880, 1881, 1883, 1887, 1888, 1891, 1893, 1898, 1900, 1902, 1903, 1904, 1905, 1907, 1910, 1911, 1913, 1914, 1916, 1917, 1920, 1922, 1923, 1924, 1925, 1926, 1927, 1928, 1931, 1932, 1936, 1937, 1938, 1940, 1941, 1943, 1944, 1945, 1946, 1947, 1948, 1952, 1953, 1954, 1956, 1957, 1964, 1967, 1969, 1970, 1973, 1978, 1981, 1982, 1983, 1984, 1985, 1992, 1995, 1996, 2000, 2001, 2003, 2004, 2006, 2012, 2017, 2018, 2019, 2020, 2021, 2023, 2025, 2028, 2029, 2030, 2032, 2033, 2035, 2038, 2042, 2043, 2046}

}

}

SET {

SEQUENCE {

INTEGER 1

SEQUENCE {

SEQUENCE {

SET {

SEQUENCE {

OBJECT IDENTIFIER 2.5.4.6

PrintableString LU

}

}

SET {

SEQUENCE {

OBJECT IDENTIFIER 2.5.4.10

PrintableString LuxTrust s.a

}

}

SET {

SEQUENCE {

OBJECT IDENTIFIER 2.5.4.3

PrintableString LuxTrust Normalised CA

```
    }
  }
}
INTEGER 2639
}
SEQUENCE {
  OBJECT IDENTIFIER 1.3.14.3.2.26
  NULL null
}
SEQUENCE {
  OBJECT IDENTIFIER 1.2.840.113549.1.1.1
  NULL null
}
OCTET STRING { 93 B2 F0 85 AF 38 06 A8 6E E6 10 94 C2 16 89 90 BD
1C 72 05 B4 E7 46 92 09 32 4A 76 E3 D4 7B 0D 8E 80 A4 46 D3 63 A2 B3 85 0A EA
41 C5 C1 D6 F2 A5 E0 64 49 6E 12 2E 52 48 D0 60 C4 FE 38 B0 C7 C9 AE 6D CE
54 E8 13 C4 09 C5 32 47 93 A7 13 9E 16 2B 2A BF EB BB 0D C9 E0 B6 5E 5C 80 21
63 B1 97 17 62 C9 D6 0A 9C C1 CB 2A F4 77 55 B9 1D 35 A4 92 48 EC F1 17 15 21
CD 39 04 3E 20 62 AD EE
}
}
}
```

The following particularities can be observed:

The version is 1.

The digest algorithms structure is empty because this information is supplied ex ante by the introductory chunk.

The encapsulated content is empty and specified by the id data object identifier.

The certificates section typically contains all certificates required for constructing a path to a trusted root. However, the signer certificate only is listed here. CRLs are omitted.

The structure contains the set of signer infos which is the essential part of the dSIG chunk containing the actual digital signature wrapped as a trailing OCTET STRING.

The signer info structure conforms to the following general syntax:

```
SignerInfo ::= SEQUENCE {
    version CMSVersion,
    sid SignerIdentifier,
    digestAlgorithm DigestAlgorithmIdentifier,
    signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
    signatureAlgorithm SignatureAlgorithmIdentifier,
    signatureValue SignatureValue,
    unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL
}

SignerIdentifier ::= CHOICE {
    issuerAndSerialNumber IssuerAndSerialNumber,
    subjectKeyIdentifier [0] SubjectKeyIdentifier
}

SignedAttributes ::= SET SIZE (1..MAX) OF Attribute
UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute

Attribute ::= SEQUENCE {
    attrType OBJECT IDENTIFIER,
    attrValues SET OF AttributeValue
}

AttributeValue ::= ANY
SignatureValue ::= OCTET STRING
```

The SignedAttrs and UnsignedAttrs are empty. The digest algorithm used is SHA-1 corresponding to the algorithm listed in the introductory chunk, The signature algorithm used is RSA.

>>

99765417 # dSIG CRC

00000000 # IEND: length 0

49454E44 # IEND

AE426082 # IEND CRC