Exemplos de certificados

Certificados X509 são documentos digitais. Eles podem estar representados em diversos formatos:

- **PEM** (*Privacy Enhanced Mail*): conteúdo codificado em base64; o arquivo costuma ter extensão `.crt`, `.pem`, `.cer` ou `.key`.
- **DER** (*Distinguished Encoding Rules*): conteúdo binário; o arquivo tem extensão `.der` ou `.cer`.
- **PKCS#7** ou **P7B**: contém um certificado e sua cadeia de certificação.
- **PKCS#12** ou **PFX**: contém um certificado, sua cadeia de certificação e a chave privada do mesmo.

Estes formatos podem ser facilmente convertidos entre si usando a ferramenta `openssl`.

UFPR

Em formato codificado PEM:

cert-ufpr.pem

```
-----BEGIN CERTIFICATE-----
MIIGUjCCBTqgAwIBAgIMVrm/K7izoJ/W11noMA0GCSqGSIb3DQEBCwUAMFAxCzAJ
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSYwJAYDVQQDEx1H
bG9iYWxTaWduIFJTQSBPViBTU0wgQ0EgMjAxODAeFw0yNTA4MjgxMjU2MDhaFw0y
NjA5MjkxMjU2MDdaMG4xCzAJBgNVBAYTAkJSMQ8wDQYDVQQIEwZQQVJBTkExETAP
BgNVBAcTCENVUklUSUJBMScwJQYDVQQKEx5VTklWRVJTSURBREUgRkVERVJBTCBE
TyBQQVJBTkExEjAQBgNVBAMMCSoudWZwci5icjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMB2NwWW/xn70scbJC5ZBp7KbQVWMPdCx3t3kbDpSCHS/BkH
Wkz420Z8z1aVufXtJ4c4DC9evue0Nz6vdWD60/+0cXomJUkOeQ7t93pxdk/I4411
Ue79uXF8pOC5x3mMGG7nlZ+cJhmgbc6Y3QMI3thFnYgxqM5nb4Kph755lfP4cgvx
l0bvHabV/UlGTUrIurfTXKg7LuUjlz/U6sb0mkuwEk59qXP1ntha16HmorUpHxCX
9/WUF/FZMKYDjlrrcJOQ+Hna5cGwdoh4Lrf7PohFHHnu0tsqPixrwQEOy3cJPotm
wYk1NrazbDzqT7i4neznXdHBe/aCalD8lOho4VMCAwEAAaOCAwwwggMIMA4GA1Ud
DwEB/wQEAwIFoDAMBgNVHRMBAf8EAjAAMIGOBggrBgEFBQcBAQSBgTB/MEQGCCsG
AQUFBzAChjhodHRwOi8vc2VjdXJlLmdsb2JhbHNpZ24uY29tL2NhY2VydC9nc3Jz
YW92c3NsY2EyMDE4LmNydDA3BggrBgEFBQcwAYYraHR0cDovL29jc3AuZ2xvYmFs
c2lnbi5jb20vZ3Nyc2FvdnNzbGNhMjAxODBWBgNVHSAETzBNMEEGCSsGAQQBoDIB
FDA0MDIGCCsGAQUFBwIBFiZodHRwczovL3d3dy5nbG9iYWxzaWduLmNvbS9yZXBv
c2l0b3J5LzAIBgZngQwBAgIwHQYDVR0RBBYwFIIJKi51ZnByLmJyggd1ZnByLmJy
MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBT473/y
zXhnqN5vjySNiPGHAwKz6zAdBgNVHQ4EFgQUDCJSa2Na48Crevj8lf2MNA5M4zAw
ggF/BgorBgEEAdZ5AgQCBIIBbwSCAWsBaQB2AJROQ4f67MHvgfMZJCaoGGUBx9Nf
OAIBP3JnfVU3LhnYAAABmPC//4QAAAQDAEcwRQIhAPIpr9dIEzaPH+hYxoSct2Dc
wyU44kdcsQHlqrb9pWpGAiB7lxiD9kklCeP4ydy4XrJIuyxGCFXQkgocvlu6nzPN
oAB3AMs49xWJfIShRF9bwd37yW7ymlnNRwppBYWwyxTDFFjnAAABmPC//d8AAAQD
AEgwRgIhAII/PuqN4CDqTCe+DH/muBJ7MnOz+d++IyZhd4Wowwb6AiEArUDVx+5E
T9mb4nkvXpQ7TaUpBhpFWD1Fc1YWGGPml8MAdgDCMX5XRRmjRe5/ON6ykEHrx8Ih
WiK/f9W1rXaa2Q5SzQAAAZjwv/9gAAAEAwBHMEUCIHK9ohRU+EcAnqaLWApeObtp
OZteIrdVW5o2fATJtM+vAiEAr9DEEBhsn3E/uvA2TC9mv0eZIJLXPXWgJ66+O1bo
3JUwDQYJKoZIhvcNAQELBQADggEBAAjYR3WP4Gt/lCASo5P04Kr2C2MmJLrZoaRQ
bOHk3bS6neUJCCAPd2AJMoaq/NElLpahHJcgN9+q1oY7XqRapFIfyfpCTcM6Pd53
sOYis4N+x0MW0/Kgi0NztEgjGuyHCcz6wI7j6qcCMVr6MoWLkSe9rLCQozr4+eJa
a5AdoOeTTrBUIbR5Ba/HFgh4SqnCi3m9QB3meENeN0Lmu8w+zULquusIGBP+6YVQ
KA5V90A+7v8co7EwWrfOY3CcHlNnkEF7POT9lzDMF6PXBcbD512NDf40h03Oy7xj
cvyDrWYN+bjGd+Ywnv3xRRI3/7n0KoE0baA/SqawXKfEfaRz+rc=
```

```
-----END CERTIFICATE-----
```

Decodificado em texto:

```
# openssl x509 -in cert-ufpr.pem -text -noout

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:b9:bf:2b:b8:b3:a0:9f:d6:d7:59:e8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
        Validity
            Not Before: Aug 28 12:56:08 2025 GMT
            Not After : Sep 29 12:56:07 2026 GMT
        Subject: C=BR, ST=PARANA, L=CURITIBA, O=UNIVERSIDADE FEDERAL DO PARANA,
CN=*.ufpr.br
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c0:76:37:05:96:ff:19:fb:d2:c7:1b:24:2e:59:
                    06:9e:ca:6d:05:56:30:f7:42:c7:7b:77:91:b0:e9:
                    48:21:d2:fc:19:07:5a:4c:f8:db:46:7c:cf:56:95:
                    b9:f5:ed:27:87:38:0c:2f:5e:be:e7:b4:37:3e:af:
                    75:60:fa:d3:ff:b4:71:7a:26:25:49:0e:79:0e:ed:
                    f7:7a:71:76:4f:c8:e3:8d:75:51:ee:fd:b9:71:7c:
                    a4:e0:b9:c7:79:8c:18:6e:e7:95:9f:9c:26:19:a0:
                    6d:ce:98:dd:03:08:de:d8:45:9d:88:31:a8:ce:67:
                    6f:82:a9:87:be:79:95:f3:f8:72:0b:f1:97:46:ef:
                    1d:a6:d5:fd:49:46:4d:4a:c8:ba:b7:d3:5c:a8:3b:
                    2e:e5:23:97:3f:d4:ea:c6:f4:9a:4b:b0:12:4e:7d:
                    a9:73:f5:9e:d8:5a:d7:a1:e6:a2:b5:29:1f:10:97:
                    f7:f5:94:17:f1:59:30:a6:03:8e:5a:eb:70:93:90:
                    f8:79:da:e5:c1:b0:76:88:78:2e:b7:fb:3e:88:45:
                    1c:79:ee:d2:db:2a:3e:2c:6b:c1:01:0e:cb:77:09:
                    3e:8b:66:c1:89:35:36:b6:b3:6c:3c:ea:4f:b8:b8:
                    9d:ec:e7:5d:d1:c1:7b:f6:82:6a:50:fc:94:e8:68:
                    e1:53
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints: critical
                CA:FALSE
            Authority Information Access:
                CA Issuers -
URI:http://secure.globalsign.com/cacert/gsrsaovsslca2018.crt
                OCSP - URI:http://ocsp.globalsign.com/gsrsaovsslca2018
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.4146.1.20
                  CPS: https://www.globalsign.com/repository/
                Policy: 2.23.140.1.2.2
            X509v3 Subject Alternative Name:
```

```
            DNS:*.ufpr.br, DNS:ufpr.br
        X509v3 Extended Key Usage:
            TLS Web Server Authentication, TLS Web Client Authentication
        X509v3 Authority Key Identifier:
            F8:EF:7F:F2:CD:78:67:A8:DE:6F:8F:24:8D:88:F1:87:03:02:B3:EB
        X509v3 Subject Key Identifier:
            0C:22:52:6B:63:5A:E3:C0:AB:7A:F8:FC:95:FD:8C:34:0E:4C:E3:30
        CT Precertificate SCTs:
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 94:4E:43:87:FA:EC:C1:EF:81:F3:19:24:26:A8:18:65:
                            01:C7:D3:5F:38:02:01:3F:72:67:7D:55:37:2E:19:D8
                Timestamp : Aug 28 12:56:11.396 2025 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:45:02:21:00:F2:29:AF:D7:48:13:36:8F:1F:E8:58:
                            C6:84:9C:B7:60:DC:C3:25:38:E2:47:5C:B1:01:E5:AA:
                            B6:FD:A5:6A:46:02:20:7B:97:18:83:F6:49:25:09:E3:
                            F8:C9:DC:B8:5E:B2:48:BB:2C:46:08:55:D0:92:0A:1C:
                            BE:5B:BA:9F:33:CD:A0
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : CB:38:F7:15:89:7C:84:A1:44:5F:5B:C1:DD:FB:C9:6E:
                            F2:9A:59:CD:47:0A:69:05:85:B0:CB:14:C3:14:58:E7
                Timestamp : Aug 28 12:56:10.975 2025 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:46:02:21:00:82:3F:3E:EA:8D:E0:20:EA:4C:27:BE:
                            0C:7F:E6:B8:12:7B:32:73:B3:F9:DF:BE:23:26:61:77:
                            85:A8:C3:06:FA:02:21:00:AD:40:D5:C7:EE:44:4F:D9:
                            9B:E2:79:2F:5E:94:3B:4D:A5:29:06:1A:45:58:3D:45:
                            73:56:16:18:63:E6:97:C3
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : C2:31:7E:57:45:19:A3:45:EE:7F:38:DE:B2:90:41:EB:
                            C7:C2:21:5A:22:BF:7F:D5:B5:AD:76:9A:D9:0E:52:CD
                Timestamp : Aug 28 12:56:11.360 2025 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:45:02:20:72:BD:A2:14:54:F8:47:00:9E:A6:8B:58:
                            0A:5E:39:BB:69:39:9B:5E:22:B7:55:5B:9A:36:7C:04:
                            C9:B4:CF:AF:02:21:00:AF:D0:C4:10:18:6C:9F:71:3F:
                            BA:F0:36:4C:2F:66:BF:47:99:20:92:D7:3D:75:A0:27:
                            AE:BE:3B:56:E8:DC:95
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        08:d8:47:75:8f:e0:6b:7f:94:20:12:a3:93:f4:e0:aa:f6:0b:
        63:26:24:ba:d9:a1:a4:50:6c:e1:e4:dd:b4:ba:9d:e5:09:08:
        20:0f:77:60:09:32:86:aa:fc:d1:25:2e:96:a1:1c:97:20:37:
        df:aa:d6:86:3b:5e:a4:5a:a4:52:1f:c9:fa:42:4d:c3:3a:3d:
        de:77:b0:e6:22:b3:83:7e:c7:43:16:d3:f2:a0:8b:43:73:b4:
        48:23:1a:ec:87:09:cc:fa:c0:8e:e3:ea:a7:02:31:5a:fa:32:
        85:8b:91:27:bd:ac:b0:90:a3:3a:f8:f9:e2:5a:6b:90:1d:a0:
        e7:93:4e:b0:54:21:b4:79:05:af:c7:16:08:78:4a:a9:c2:8b:
        79:bd:40:1d:e6:78:43:5e:37:42:e6:bb:cc:3e:cd:42:ea:ba:
        eb:08:18:13:fe:e9:85:50:28:0e:55:f7:40:3e:ee:ff:1c:a3:
```

```
        b1:30:5a:b7:ce:63:70:9c:1e:53:67:90:41:7b:3c:e4:fd:97:
        30:cc:17:a3:d7:05:c6:c3:e7:5d:8d:0d:fe:34:87:4d:ce:cb:
        bc:63:72:fc:83:ad:66:0d:f9:b8:c6:77:e6:30:9e:fd:f1:45:
        12:37:ff:b9:f4:2a:81:34:6d:a0:3f:4a:a6:b0:5c:a7:c4:7d:
        a4:73:fa:b7
```

Banco do Brasil

Em formato codificado PEM:

cert-bb.pem

```
-----BEGIN CERTIFICATE-----
MIIHGzCCBgOgAwIBAgIQBseoHNrdzNm1hYMPX/rBBDANBgkqhkiG9w0BAQsFADBE
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMR4wHAYDVQQDExVH
ZW9UcnVzdCBFViBSU0EgQ0EgRzIwHhcNMjYwNzI5MDAwMDAwWhcNMjcwMjEyMjM1
OTU5WjCBwzETMBEGCysGAQQBgjc8AgEDEwJCUjEdMBsGA1UEDwwUUHJpdmF0ZSBP
cmdhbml6YXRpb24xGzAZBgNVBAUTEjAwLjAwMC4wMDAvMDAwMS05MTELMAkGA1UE
BhMCQlIxGTAXBgNVBAgTEERpc3RyaXRvIEZlZGVyYWwxETAPBgNVBAcTCEJyYXNp
bGlhMR0wGwYDVQQKExRCQU5DTyBETyBCUkFTSUwgUy5BLjEWMBQGA1UEAxMNd3d3
LmJiLmNvbS5icjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJzw3Lsa
wqVg7py9eny+ttcsyQjHGvOXQvwvQe8jLK710xgep2vYQ2ce4fIuYIppOHxmmnDa
RdiCWTVvEwiwxe284HS62/0OPxDRWvOd/+WcavJhRvGdB/UufOxVqSbPmRnpNcP9
mWcJYYohFTu/tYZC7tBGivnvjfDCu4DofJTnwfNSOFChr7RVJ8YvcwX3qIDznrKq
HAFsSY3dSZU5y3O/x3QjNaCteH5JX1YI8lkf2CfnKt10CdtXa2ljYE694z85F2yz
+2hkjRf14pk+86VKErITXIEiLsRXiQJZNvcPAVjKGbSl9/z7ka1krnkx1LtksfEH
0Vu2UOya7sBpu+cCAwEAAaOCA4cwggODMB8GA1UdIwQYMBaAFCjSz+4JhHXdtbK1
vzzVoMZziF0fMB0GA1UdDgQWBBTL/woaXUvyYXKngbk/0zGdMX3VWTBVBgNVHREE
TjBMgg13d3cuYmIuY29tLmJyggliYi5jb20uYnKCFnd3dy5iYW5jb2JyYXNpbC5j
b20uYnKCGHd3dy5iYW5jb2RvYnJhc2lsLmNvbS5icjBKBgNVHSAEQzBBMAsGCWCG
SAGG/WwCATAyBgVngQwBATApMCcGCCsGAQUFBwIBFhtodHRwOi8vd3d3LmRpZ2lj
ZXJ0LmNvbS9DUFMwDgYDVR0PAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMB
MHUGA1UdHwRuMGwwNKAyoDCGLmh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9HZW9U
cnVzdEVWUlNBQ0FHMi5jcmwwNKAyoDCGLmh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNv
bS9HZW9UcnVzdEVWUlNBQ0FHMi5jcmwwcwYIKwYBBQUHAQEEZzBlMCQGCCsGAQUF
BzABhhhodHRwOi8vb2NzcC5kaWdpY2VydC5jb20wPQYIKwYBBQUHMAKGMWh0dHA6
Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9HZW9UcnVzdEVWUlNBQ0FHMi5jcnQwDAYD
VR0TAQH/BAIwADCCAX0GCisGAQQB1nkCBAIEggFtBIIBaQFnAHUATGPcmOWcHauI
9h6KPd6uj6tEozd7X5uUw/uhnPzBviYAAAGfrucUGAAABAMARjBEAiBl7v7E6F6W
O6/nDQQ25LjgaHRRNlo5lrbDDlowKuNRugIgDDAcqvV2pgKHbmjAMiz5cXKfIPM0
vOeaz9RsZafe8bcAdgDW1Y2p0BdT82pKoMdXSQKv68fcLNOM2fdkyAyJGR6fAgAA
AZ+u5xQpAAAEAwBHMEUCIQDTZYwwS2JfhfpP8+HPIs7fVbsfKtI9BEoKldpZ9sun
pAIgaegi3lFnk82buQ+9oUBYe37DeWoBVgx3n8B18o0RjHIAdgAcn2gs6frwRWlQ
+BuWiofd2zIQ2EzmyLLjglJKxM9ZnwAAAZ+u5xS7AAAEAwBHMEUCIQClzBB0embf
IT7Wsfty/2G3k3f5GH47GrZqT/wHATkacwIgIPUVcoKWWHqSeDux9XQoAVrlZohC
tkTDw13r0Ejb3r8wDQYJKoZIhvcNAQELBQADggEBAD2B+lTC3RxGNGDhG0K0Dfdl
V35BaHW9+FU3g7GM5IdDlSPSYDLmerulocdeNP95iH/RYup3JKdrwk/p3vuwnmLQ
7dg72Usym2KMH/9hdxChL+gVUHtq1GlrUpXFAKb87/Qy8qkpMBgUmoy05Eq7QLla
+Ar6LdiLfFKN9OtC8BiODyUZFXmvYCRmvZ1Sltm/WCZKp+Hm7riIET5RU6b2d3Fk
Jyhj0qKYlEvuDbvf6glEcmhuokJ5oukP1ORslB2PAc3FAi8f7bSM76K3la0MKYfC
ttxbtAyRFQpx0g4bdbjGjHJcz+Lx+uTtjDT+tFuZttWEjzha8MbgoOyZn/NjStQ=
-----END CERTIFICATE-----
```

Decodificado em texto:

```
# openssl x509 -in cert-bb.pem -text -noout

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            06:c7:a8:1c:da:dd:cc:d9:b5:85:83:0f:5f:fa:c1:04
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, CN=GeoTrust EV RSA CA G2
        Validity
            Not Before: Jul 29 00:00:00 2026 GMT
            Not After : Feb 12 23:59:59 2027 GMT
        Subject: jurisdictionC=BR, businessCategory=Private Organization,
serialNumber=00.000.000/0001-91, C=BR, ST=Distrito Federal, L=Brasilia, O=BANCO DO
BRASIL S.A., CN=www.bb.com.br
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9c:f0:dc:bb:1a:c2:a5:60:ee:9c:bd:7a:7c:be:
                    b6:d7:2c:c9:08:c7:1a:f3:97:42:fc:2f:41:ef:23:
                    2c:ae:f5:d3:18:1e:a7:6b:d8:43:67:1e:e1:f2:2e:
                    60:8a:69:38:7c:66:9a:70:da:45:d8:82:59:35:6f:
                    13:08:b0:c5:ed:bc:e0:74:ba:db:fd:0e:3f:10:d1:
                    5a:f3:9d:ff:e5:9c:6a:f2:61:46:f1:9d:07:f5:2e:
                    7c:ec:55:a9:26:cf:99:19:e9:35:c3:fd:99:67:09:
                    61:8a:21:15:3b:bf:b5:86:42:ee:d0:46:8a:f9:ef:
                    8d:f0:c2:bb:80:e8:7c:94:e7:c1:f3:52:38:50:a1:
                    af:b4:55:27:c6:2f:73:05:f7:a8:80:f3:9e:b2:aa:
                    1c:01:6c:49:8d:dd:49:95:39:cb:73:bf:c7:74:23:
                    35:a0:ad:78:7e:49:5f:56:08:f2:59:1f:d8:27:e7:
                    2a:dd:74:09:db:57:6b:69:63:60:4e:bd:e3:3f:39:
                    17:6c:b3:fb:68:64:8d:17:f5:e2:99:3e:f3:a5:4a:
                    12:b2:13:5c:81:22:2e:c4:57:89:02:59:36:f7:0f:
                    01:58:ca:19:b4:a5:f7:fc:fb:91:ad:64:ae:79:31:
                    d4:bb:64:b1:f1:07:d1:5b:b6:50:ec:9a:ee:c0:69:
                    bb:e7
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                28:D2:CF:EE:09:84:75:DD:B5:B2:B5:BF:3C:D5:A0:C6:73:88:5D:1F
            X509v3 Subject Key Identifier:
                CB:FF:0A:1A:5D:4B:F2:61:72:A7:81:B9:3F:D3:31:9D:31:7D:D5:59
            X509v3 Subject Alternative Name:
                DNS:www.bb.com.br, DNS:bb.com.br, DNS:www.bancobrasil.com.br,
DNS:www.bancodobrasil.com.br
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114412.2.1
                Policy: 2.23.140.1.1
                  CPS: http://www.digicert.com/CPS
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 CRL Distribution Points:
                Full Name:
```

```
                URI:http://crl3.digicert.com/GeoTrustEVRSACAG2.crl

            Full Name:
              URI:http://crl4.digicert.com/GeoTrustEVRSACAG2.crl

        Authority Information Access:
            OCSP - URI:http://ocsp.digicert.com
            CA Issuers - URI:http://cacerts.digicert.com/GeoTrustEVRSACAG2.crt
        X509v3 Basic Constraints: critical
            CA:FALSE
        CT Precertificate SCTs:
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 4C:63:DC:98:E5:9C:1D:AB:88:F6:1E:8A:3D:DE:AE:8F:
                            AB:44:A3:37:7B:5F:9B:94:C3:FB:A1:9C:FC:C1:BE:26
                Timestamp : Jul 29 17:23:27.384 2026 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:44:02:20:65:EE:FE:C4:E8:5E:96:3B:AF:E7:0D:04:
                            36:E4:B8:E0:68:74:51:36:5A:39:96:B6:C3:0E:5A:30:
                            2A:E3:51:BA:02:20:0C:30:1C:AA:F5:76:A6:02:87:6E:
                            68:C0:32:2C:F9:71:72:9F:20:F3:34:BC:E7:9A:CF:D4:
                            6C:65:A7:DE:F1:B7
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : D6:D5:8D:A9:D0:17:53:F3:6A:4A:A0:C7:57:49:02:AF:
                            EB:C7:DC:2C:D3:8C:D9:F7:64:C8:0C:89:19:1E:9F:02
                Timestamp : Jul 29 17:23:27.401 2026 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:45:02:21:00:D3:65:8C:30:4B:62:5F:85:FA:4F:F3:
                            E1:CF:22:CE:DF:55:BB:1F:2A:D2:3D:04:4A:0A:95:DA:
                            59:F6:CB:A7:A4:02:20:69:E8:22:DE:51:67:93:CD:9B:
                            B9:0F:BD:A1:40:58:7B:7E:C3:79:6A:01:56:0C:77:9F:
                            C0:75:F2:8D:11:8C:72
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 1C:9F:68:2C:E9:FA:F0:45:69:50:F8:1B:96:8A:87:DD:
                            DB:32:10:D8:4C:E6:C8:B2:E3:82:52:4A:C4:CF:59:9F
                Timestamp : Jul 29 17:23:27.547 2026 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:45:02:21:00:A5:CC:10:74:7A:66:DF:21:3E:D6:B1:
                            FB:72:FF:61:B7:93:77:F9:18:7E:3B:1A:B6:6A:4F:FC:
                            07:01:39:1A:73:02:20:20:F5:15:72:82:96:58:7A:92:
                            78:3B:B1:F5:74:28:01:5A:E5:66:88:42:B6:44:C3:C3:
                            5D:EB:D0:48:DB:DE:BF
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        3d:81:fa:54:c2:dd:1c:46:34:60:e1:1b:42:b4:0d:f7:65:57:
        7e:41:68:75:bd:f8:55:37:83:b1:8c:e4:87:43:95:23:d2:60:
        32:e6:7a:bb:a5:a1:c7:5e:34:ff:79:88:7f:d1:62:ea:77:24:
        a7:6b:c2:4f:e9:de:fb:b0:9e:62:d0:ed:d8:3b:d9:4b:32:9b:
        62:8c:1f:ff:61:77:10:a1:2f:e8:15:50:7b:6a:d4:69:6b:52:
        95:c5:00:a6:fc:ef:f4:32:f2:a9:29:30:18:14:9a:8c:b4:e4:
        4a:bb:40:b9:5a:f8:0a:fa:2d:d8:8b:7c:52:8d:f4:eb:42:f0:
```

```
        18:8e:0f:25:19:15:79:af:60:24:66:bd:9d:52:96:d9:bf:58:
        26:4a:a7:e1:e6:ee:b8:88:11:3e:51:53:a6:f6:77:71:64:27:
        28:63:d2:a2:98:94:4b:ee:0d:bb:df:ea:09:44:72:68:6e:a2:
        42:79:a2:e9:0f:d4:e4:6c:94:1d:8f:01:cd:c5:02:2f:1f:ed:
        b4:8c:ef:a2:b7:95:ad:0c:29:87:c2:b6:dc:5b:b4:0c:91:15:
        0a:71:d2:0e:1b:75:b8:c6:8c:72:5c:cf:e2:f1:fa:e4:ed:8c:
        34:fe:b4:5b:99:b6:d5:84:8f:38:5a:f0:c6:e0:a0:ec:99:9f:
        f3:63:4a:d4
```

From:
https://wiki.inf.ufpr.br/maziero/ - **Prof. Carlos Maziero**

Permanent link:
https://wiki.inf.ufpr.br/maziero/doku.php?id=sc:exemplos_de_certificados

Last update: **2026/08/19 10:54**