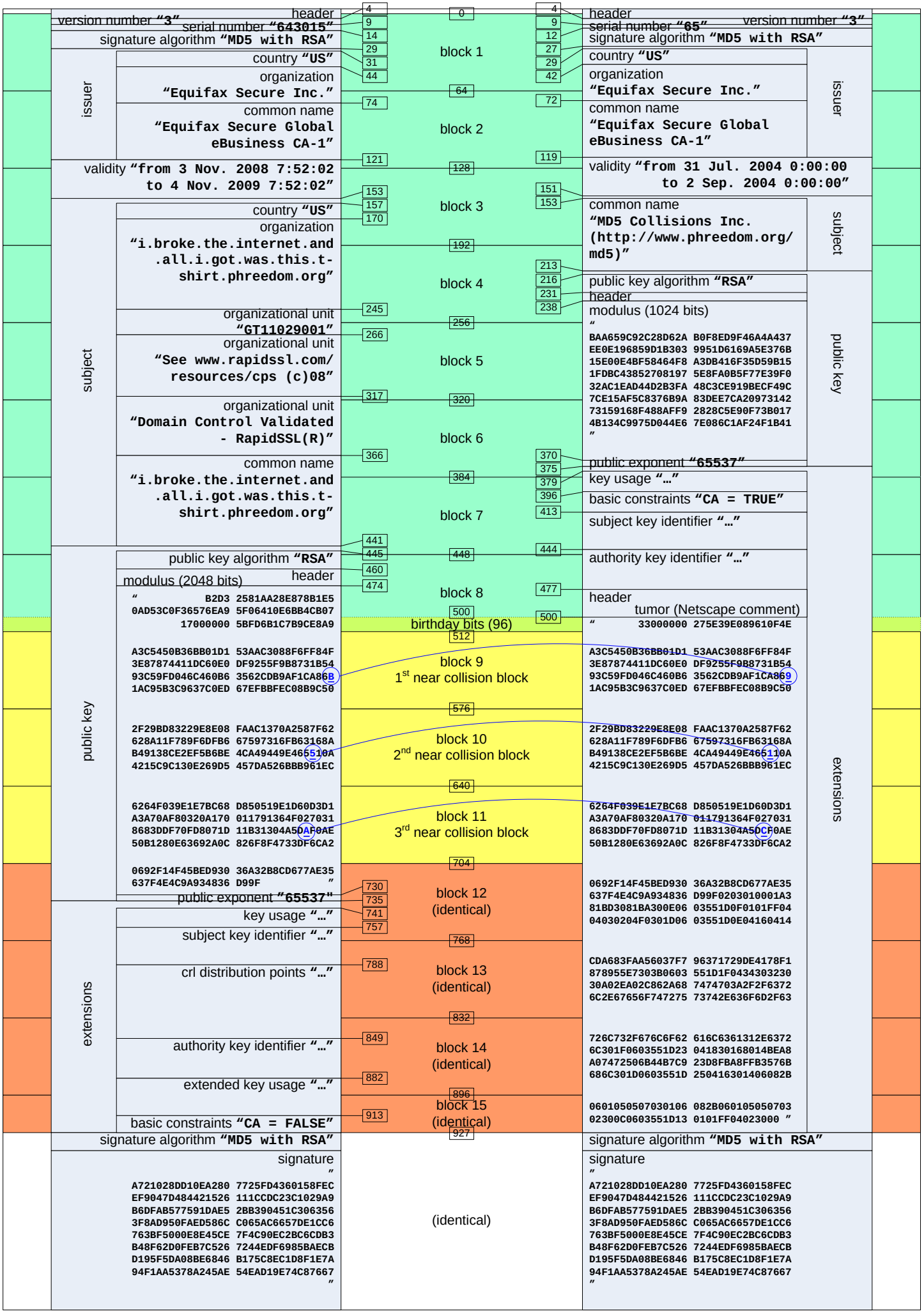
real certificate
rogue CA certificate
header
version number "3"
serial number "643015"
signature algorithm "MD5 with RSA"
issuer
country "US"
organization "Equifax Secure Inc."
common name "Equifax Secure Global eBusiness CA-1"
validity "from 3 Nov. 2008 7:52:02 to 4 Nov. 2009 7:52:02"
subject
country "US"
organization "i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org"
organizational unit "GT11029001"
organizational unit "See www.rapidssl.com/resources/cps (c)08"
organizational unit "Domain Control Validated - RapidSSL(R)"
common name "i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org"
public key
public key algorithm "RSA"
header
modulus (2048 bits)
" B2D3 2581AA28E878B1E5
0AD53C0F36576EA9 5F06410E6BB4CB07
17000000 5BFD6B1C7B9CE8A9
A3C5450B36BB01D1 53AAC3088F6FF84F
3E87874411DC60E0 DF9255F9B8731B54
93C59FD046C460B6 3562CDB9AF1CA86B
1AC95B3C9637C0ED 67EFBBFEC08B9C50
2F29BD83229E8E08 FAAC1370A2587F62
628A11F789F6DFB6 67597316FB63168A
B49138CE2EF5B6BE 4CA49449E465510A
4215C9C130E269D5 457DA526BBB961EC
6264F039E1E7BC68 D850519E1D60D3D1
A3A70AF80320A170 011791364F027031
8683DDF70FD8071D 11B31304A5DAF0AE
50B1280E63692A0C 826F8F4733DF6CA2
0692F14F45BED930 36A32B8CD677AE35
637F4E4C9A934836 D99F "
public exponent "65537"
extensions
key usage "..."
subject key identifier "..."
crl distribution points "..."
authority key identifier "..."
extended key usage "..."
basic constraints "CA = FALSE"
signature algorithm "MD5 with RSA"
signature
"
A721028DD10EA280 7725FD4360158FEC
EF9047D484421526 111CCDC23C1029A9
B6DFAB577591DAE5 2BB390451C306356
3F8AD950FAED586C C065AC6657DE1CC6
763BF5000E8E45CE 7F4C90EC2BC6CDB3
B48F62D0FEB7C526 7244EDF6985BAECB
D195F5DA08BE6846 B175C8EC1D8F1E7A
94F1AA5378A245AE 54EAD19E74C87667
"
block 1
block 2
block 3
block 4
block 5
block 6
block 7
block 8
birthday bits (96)
block 9
1st near collision block
block 10
2nd near collision block
block 11
3rd near collision block
block 12
(identical)
block 13
(identical)
block 14
(identical)
block 15
(identical)
(identical)
header
version number "3"
serial number "65"
signature algorithm "MD5 with RSA"
issuer
country "US"
organization "Equifax Secure Inc."
common name "Equifax Secure Global eBusiness CA-1"
validity "from 31 Jul. 2004 0:00:00 to 2 Sep. 2004 0:00:00"
subject
common name "MD5 Collisions Inc. (http://www.phreedom.org/md5)"
public key
public key algorithm "RSA"
header
modulus (1024 bits)
"
BAA659C92C28D62A B0F8ED9F46A4A437
EE0E196859D1B303 9951D6169A5E376B
15E00E4BF58464F8 A3DB416F35D59B15
1FDBC43852708197 5E8FA0B5F77E39F0
32AC1EAD44D2B3FA 48C3CE919BECF49C
7CE15AF5C8376B9A 83DEE7CA20973142
73159168F488AFF9 2828C5E90F73B017
4B134C9975D044E6 7E086C1AF24F1B41
"
public exponent "65537"
extensions
key usage "..."
basic constraints "CA = TRUE"
subject key identifier "..."
authority key identifier "..."
header
tumor (Netscape comment)
" 33000000 275E39E089610F4E
A3C5450B36BB01D1 53AAC3088F6FF84F
3E87874411DC60E0 DF9255F9B8731B54
93C59FD046C460B6 3562CDB9AF1CA869
1AC95B3C9637C0ED 67EFBBFEC08B9C50
2F29BD83229E8E08 FAAC1370A2587F62
628A11F789F6DFB6 67597316FB63168A
B49138CE2EF5B6BE 4CA49449E465110A
4215C9C130E269D5 457DA526BBB961EC
6264F039E1E7BC68 D850519E1D60D3D1
A3A70AF80320A170 011791364F027031
8683DDF70FD8071D 11B31304A5DCF0AE
50B1280E63692A0C 826F8F4733DF6CA2
0692F14F45BED930 36A32B8CD677AE35
637F4E4C9A934836 D99F0203010001A3
81BD3081BA300E06 03551D0F0101FF04
04030204F0301D06 03551D0E04160414
CDA683FAA56037F7 96371729DE4178F1
878955E7303B0603 551D1F0434303230
30A02EA02C862A68 7474703A2F2F6372
6C2E67656F747275 73742E636F6D2F63
726C732F676C6F62 616C6361312E6372
6C301F0603551D23 041830168014BEA8
A07472506B44B7C9 23D8FBA8FFB3576B
686C301D0603551D 250416301406082B
0601050507030106 082B060105050703
02300C0603551D13 0101FF04023000 "
signature algorithm "MD5 with RSA"
signature
"
A721028DD10EA280 7725FD4360158FEC
EF9047D484421526 111CCDC23C1029A9
B6DFAB577591DAE5 2BB390451C306356
3F8AD950FAED586C C065AC6657DE1CC6
763BF5000E8E45CE 7F4C90EC2BC6CDB3
B48F62D0FEB7C526 7244EDF6985BAECB
D195F5DA08BE6846 B175C8EC1D8F1E7A
94F1AA5378A245AE 54EAD19E74C87667
"