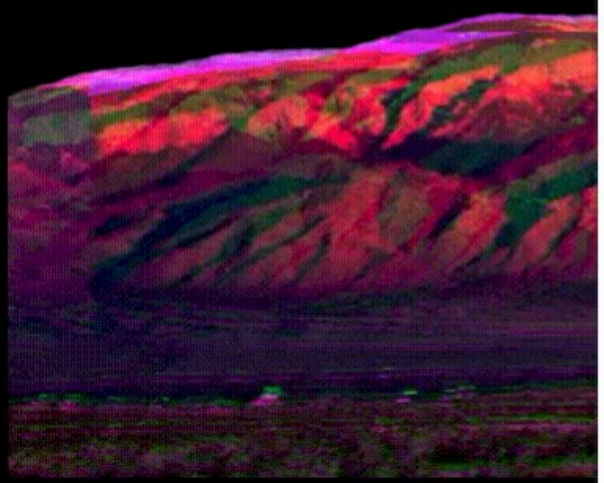
Notes about rogue cert paper...

Home -

breakpointingbad.com

BREAKPOINT BAD



We are a non-profit founded in 20 ut

combined experience focusing on

goal is to provide technical expertise and capabilities to at-risk populations subjected t

Certificate Viewer: breakpointingbad.com

General | Details

Issued To

Common Name (CN)	breakpointingbad.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

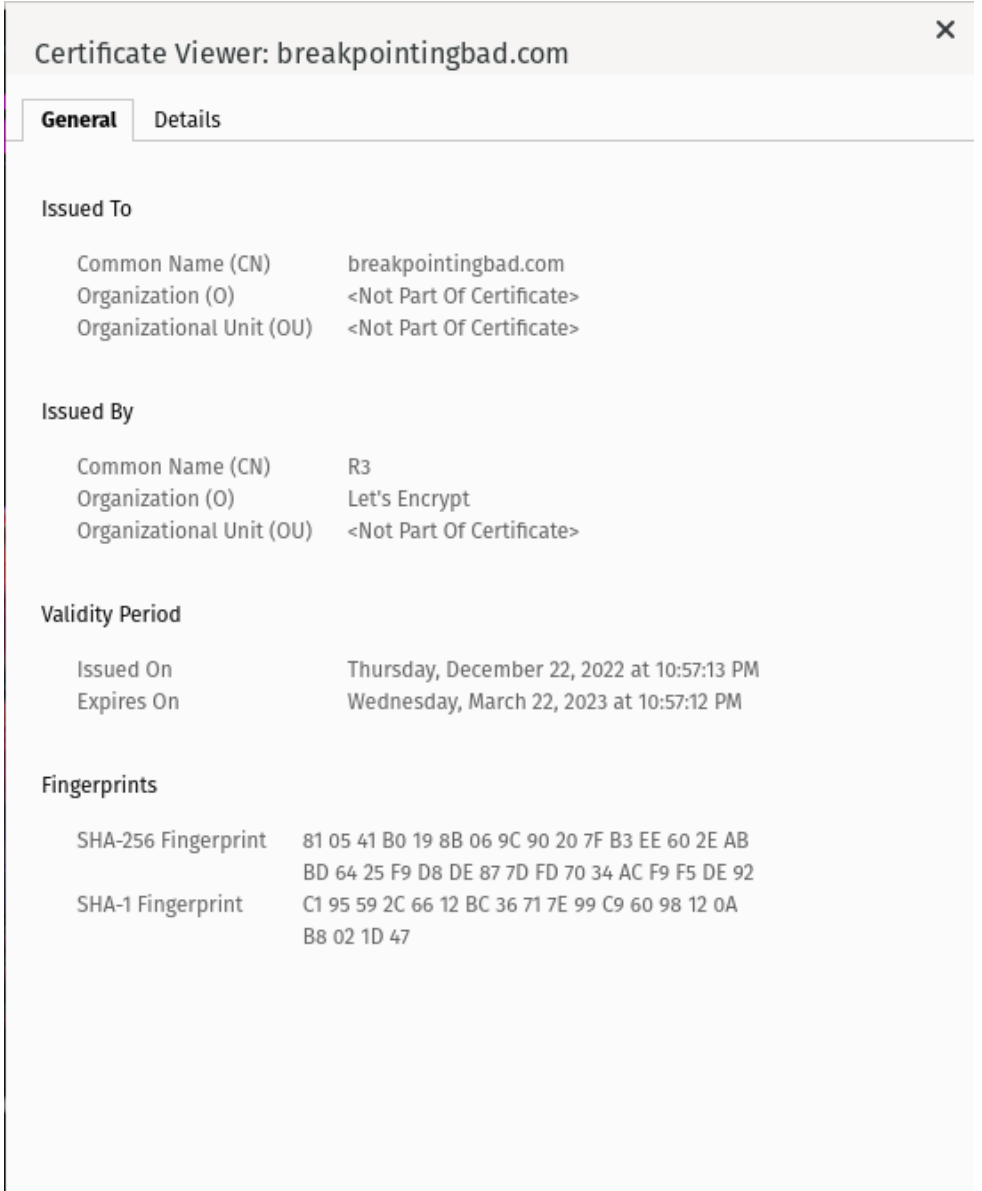
Common Name (CN)	R3
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Thursday, December 22, 2022 at 10:57:13 PM
Expires On	Wednesday, March 22, 2023 at 10:57:12 PM

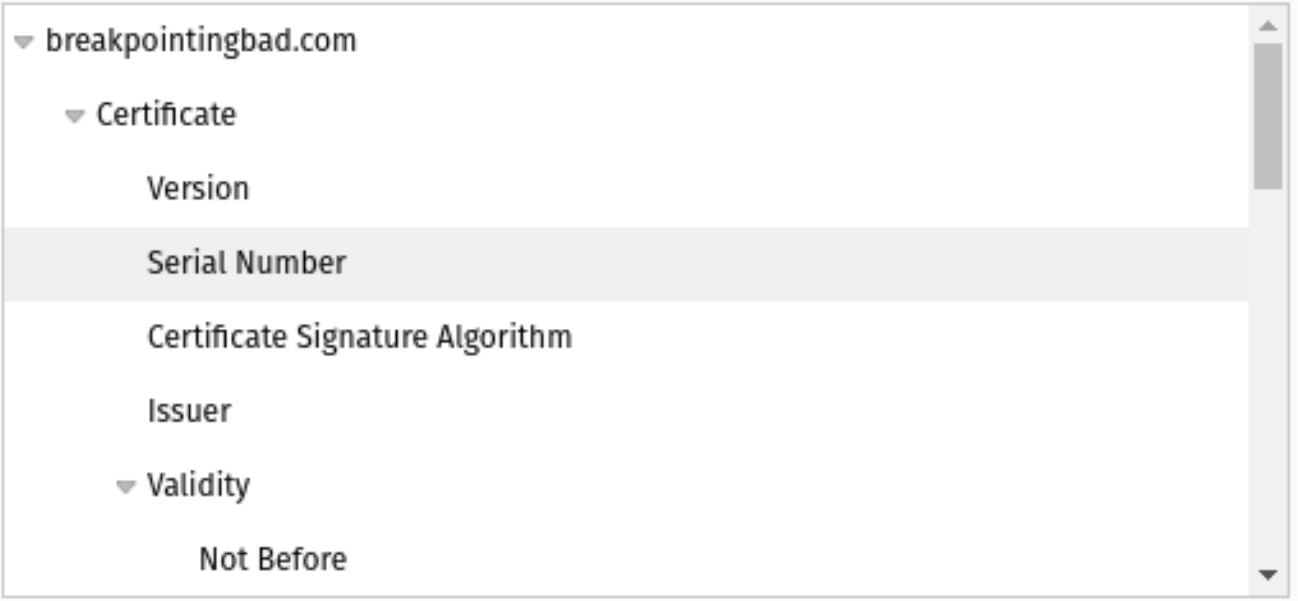
Fingerprints

SHA-256 Fingerprint	81 05 41 B0 19 8B 06 9C 90 20 7F B3 EE 60 2E AB BD 64 25 F9 D8 DE 87 7D FD 70 34 AC F9 F5 DE 92
SHA-1 Fingerprint	C1 95 59 2C 66 12 BC 36 71 7E 99 C9 60 98 12 0A B8 02 1D 47


Certificate Viewer: breakpointingbad.com
General
Details
Issued To
Common Name (CN) breakpointingbad.com
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) R3
Organization (O) Let's Encrypt
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Thursday, December 22, 2022 at 10:57:13 PM
Expires On Wednesday, March 22, 2023 at 10:57:12 PM
Fingerprints
SHA-256 Fingerprint 81 05 41 B0 19 8B 06 9C 90 20 7F B3 EE 60 2E AB BD 64 25 F9 D8 DE 87 7D FD 70 34 AC F9 F5 DE 92
SHA-1 Fingerprint C1 95 59 2C 66 12 BC 36 71 7E 99 C9 60 98 12 0A B8 02 1D 47

breakpointingbad.com

Certificate Fields



Field Value

04:B5:2A:1D:FD:B3:AC:F1:34:37:27:94:9F:F5:A8:5A:12:E6

Export...

breakpointingbad.com

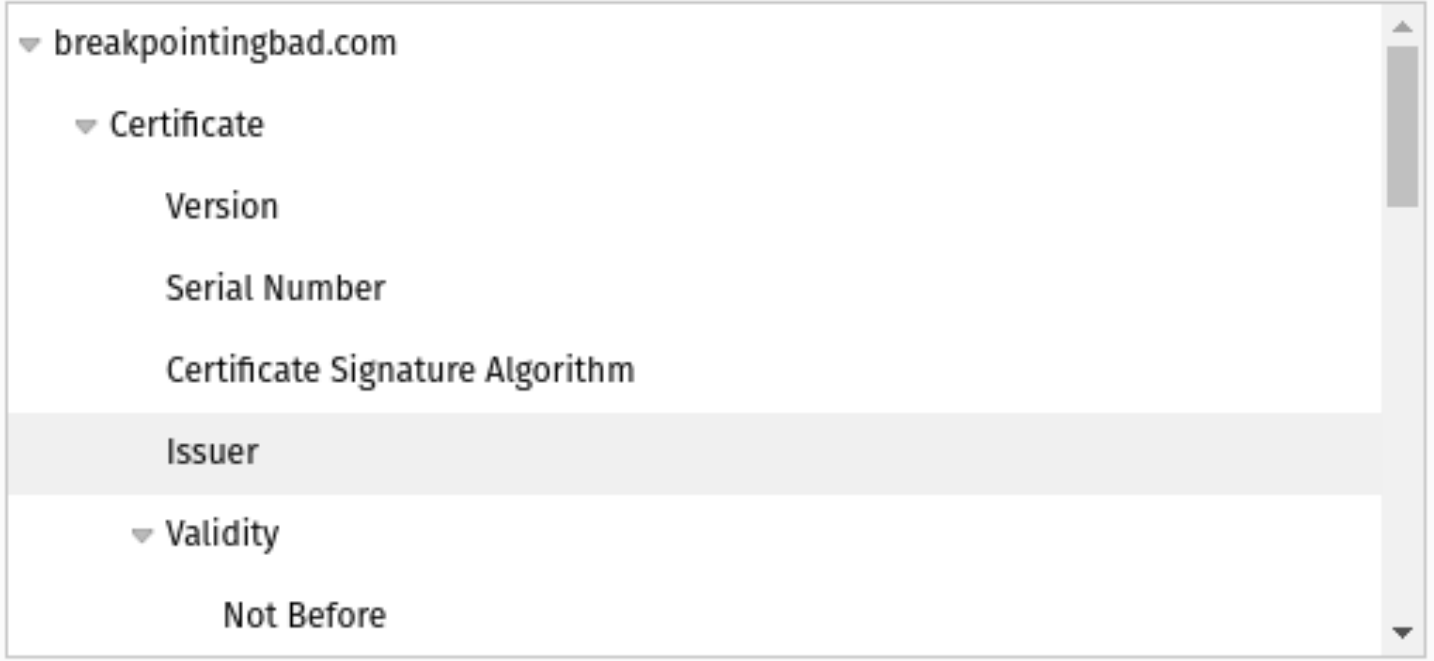
Certificate Fields

- breakpointingbad.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

Field Value

PKCS #1 SHA-256 With RSA Encryption

Certificate Fields



Field Value

CN = R3
O = Let's Encrypt
C = US

breakpointingbad.com

Certificate Fields

Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Subject Public Key Algorithm

Field Value

3/22/23, 10:57:12 PM MST

Export...

breakpointingbad.com

Certificate Fields

Certificate Signature Algorithm

Issuer

Validity

Not Before

Not After

Subject

Subject Public Key Info

Subject Public Key Algorithm

Field Value

CN = breakpointingbad.com

breakpointingbad.com

Certificate Fields

Not After

Subject

Subject Public Key Info

Subject Public Key Algorithm

Subject's Public Key

Extensions

Certificate Key Usage

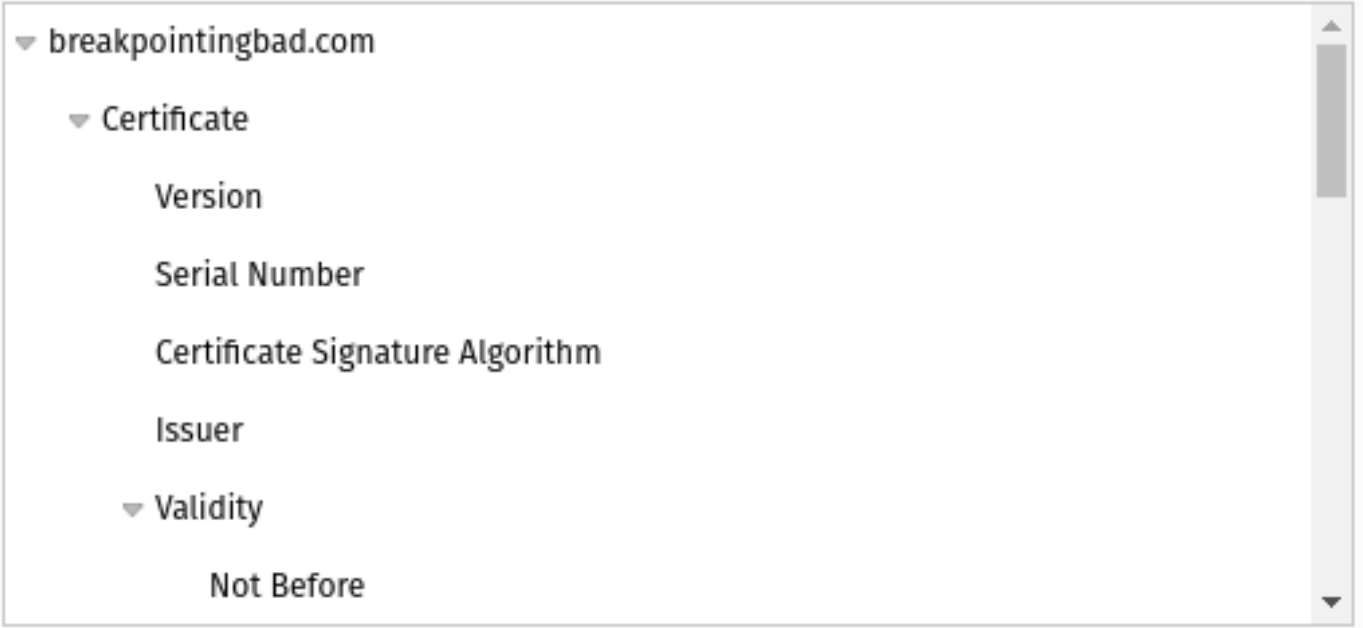
Extended Key Usage

Field Value

Modulus (2048 bits):
DC DA F0 96 47 5C 62 91 27 27 AD B2 95 EE 3D 51
CF 26 EB EC 27 EE ED 2E 9F DA 1D BF 83 2F 12 F0
EA CC 96 5B 8C C1 3E A1 C6 46 90 4D E5 93 20 E1
5C 9B 62 BB 82 3A 7F 77 7C 85 CB 8C F3 0F B9 0D
38 24 9C 0D 39 8C FF F4 B5 AD 0A 94 75 AA F9 41

Export...

Certificate Fields



Field Value

Export...

Certificate Hierarchy

- Builtin Object Token:ISRG Root X1
  - R3
    - breakpointingbad.com

Certificate Fields

- Subject's Public Key
- Extensions
  - Certificate Key Usage
  - Extended Key Usage
  - Certificate Basic Constraints
  - Certificate Subject Key ID
  - Certification Authority Key ID
  - Authority Information Access

Field Value

Critical
Is not a Certification Authority

R3

breakpointingbad.com

Certificate Fields

Certificate Subject Alternative Name

Certificate Policies

OID.1.3.6.1.4.1.11129.2.4.2

Certificate Signature Algorithm

Certificate Signature Value

Fingerprints

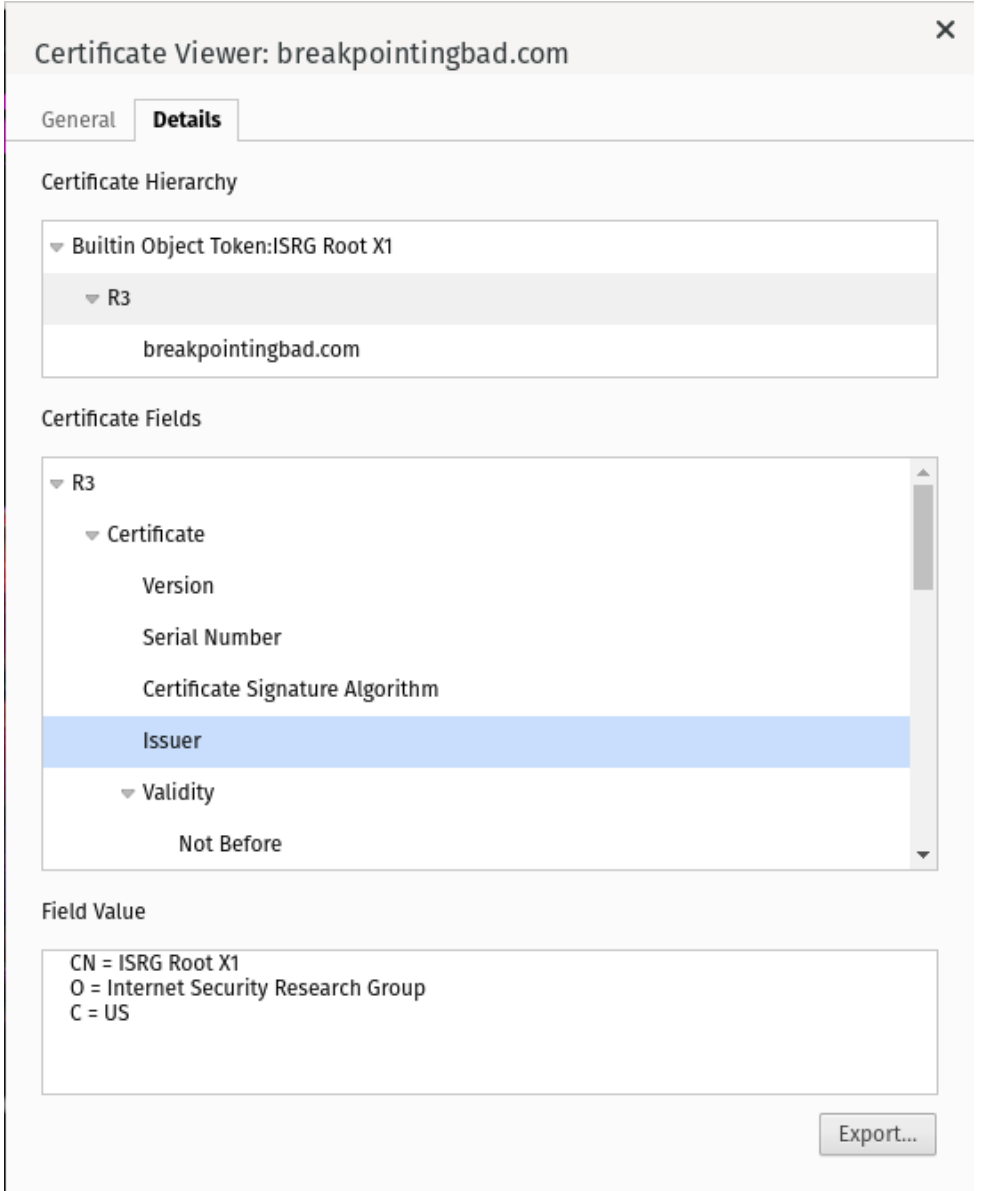
SHA-256 Fingerprint

SHA-1 Fingerprint

Field Value

81 05 41 B0 19 8B 06 9C 90 20 7F B3 EE 60 2E AB
BD 64 25 F9 D8 DE 87 7D FD 70 34 AC F9 F5 DE 92

Export


Certificate Viewer: breakpointingbad.com
General
Details
Certificate Hierarchy
Builtin Object Token:ISRG Root X1
R3
breakpointingbad.com
Certificate Fields
R3
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Field Value
CN = ISRG Root X1
O = Internet Security Research Group
C = US
Export...

R3

breakpointingbad.com

Certificate Fields

R3

Certificate

Version

Serial Number

Certificate Signature Algorithm

Issuer

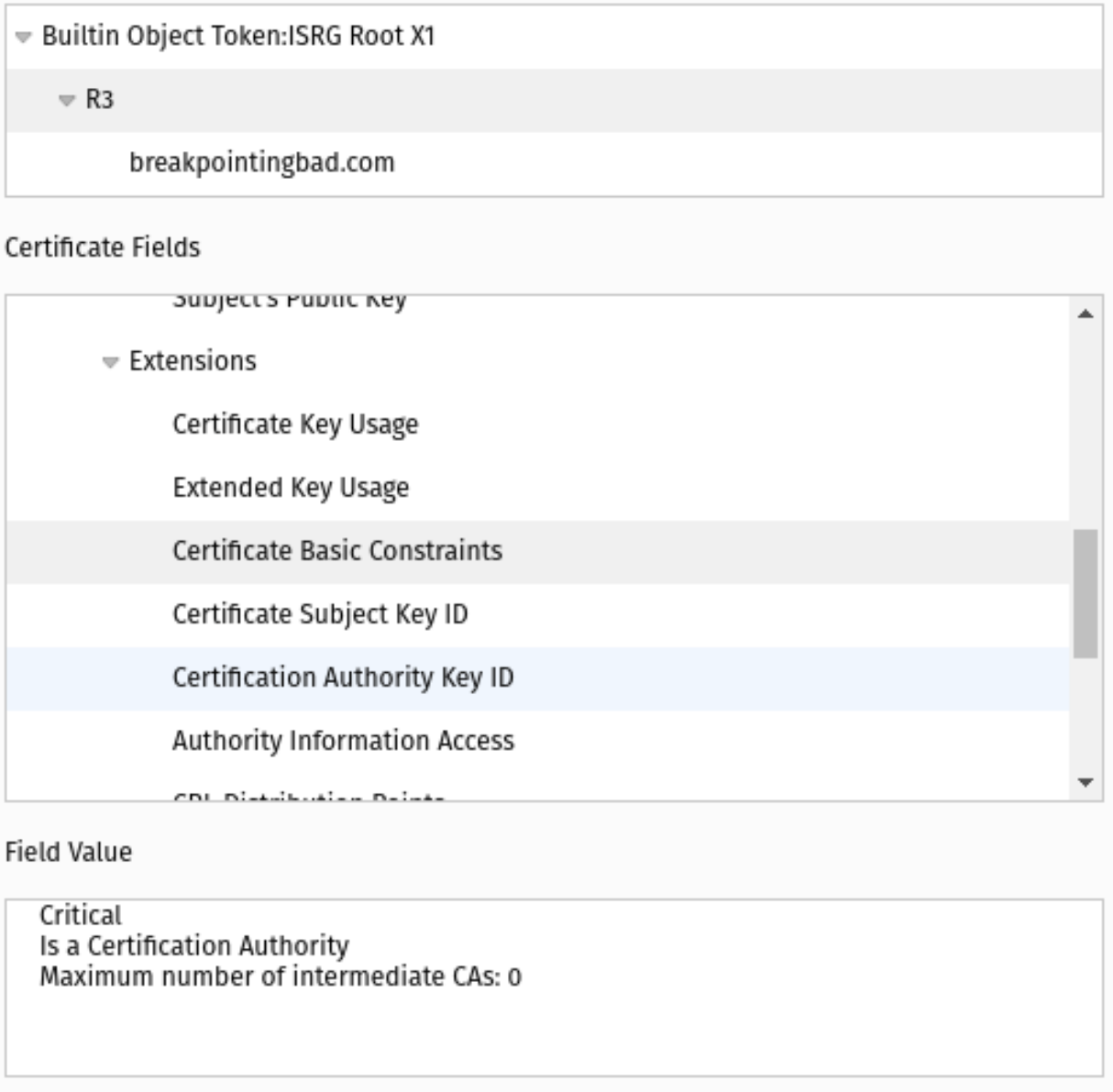
Validity

Not Before

Field Value

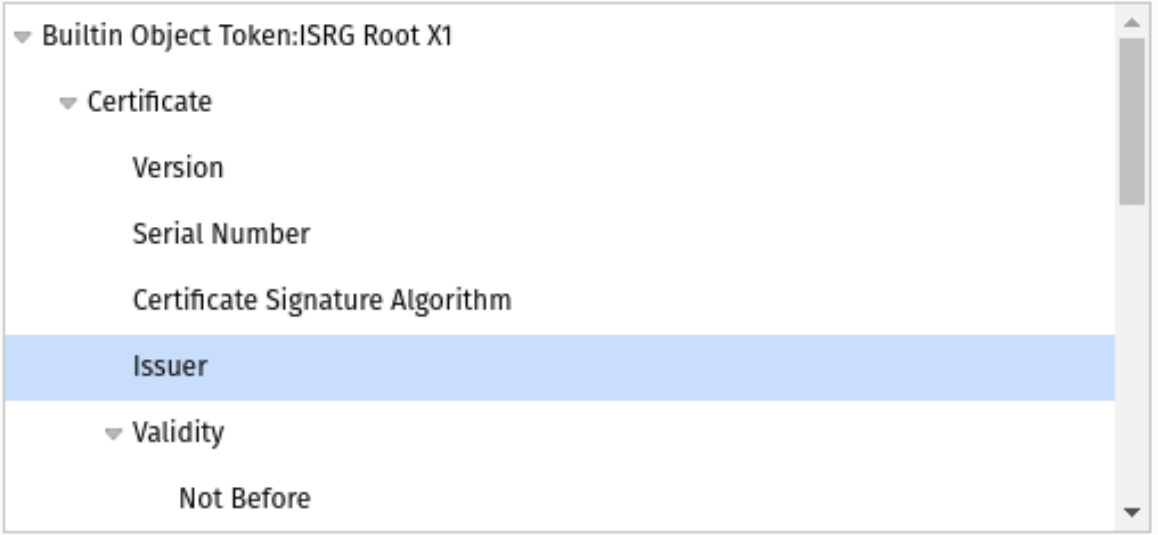
CN = ISRG Root X1
O = Internet Security Research Group
C = US

Export...

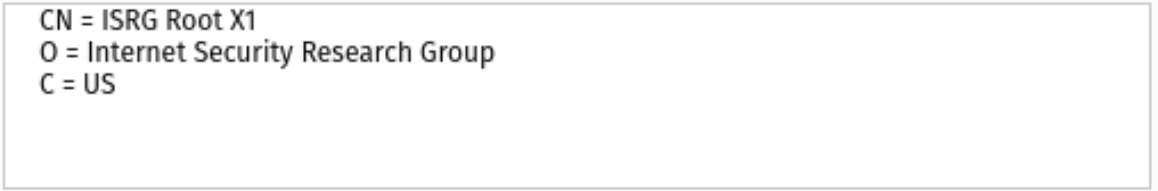

Builtin Object Token:ISRG Root X1
R3
breakpointingbad.com
Certificate Fields
Extensions
Certificate Key Usage
Extended Key Usage
Certificate Basic Constraints
Certificate Subject Key ID
Certification Authority Key ID
Authority Information Access
Field Value
Critical
Is a Certification Authority
Maximum number of intermediate CAs: 0

Certificate Hierarchy

Certificate Fields



Field Value



Builtin Object Token:ISRG Root X1

R3

breakpointingbad.com

Certificate Fields

Subject's Public Key

Extensions

Certificate Key Usage

Certificate Basic Constraints

Certificate Subject Key ID

Certificate Signature Algorithm

Certificate Signature Value

Fingerprints

Field Value

Critical
Is a Certification Authority
Maximum number of intermediate CAs: unlimited

Export...

Privacy and security
Appearance
Search engine
Default browser
On startup
Languages
Downloads
Accessibility
System
Reset settings
Extensions
About Chromium

org-GlobalSign nv-sa

org-GoDaddy.com, Inc.

org-Google Trust Services LLC

org-Government Root Certification Authority

org-GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.

org-Hellenic Academic and Research Institutions Cert. Authority

org-Hongkong Post

org-IdenTrust

org-Internet Security Research Group

org-IZENPE S.A.

org-Japan Certification Services, Inc.

org-Krajowa Izba Rozliczeniowa S.A.

org-LuxTrust S.A.

https://www.win.tue.nl/hashclash/rogue-ca/

Creating an intermediate CA

https://www.win.tue.nl/hashclash/rogue-ca/downloads/md5-collisions-1.0.pdf