## 获取路径

[(16条消息) 公钥证书简介\_anniesqq的博客-CSDN博客\_公钥证书](https://blog.csdn.net/weixin_42534168/article/details/115712212)（在浏览器的地址栏旁边的小锁中导出）

各字段意义

|  |  |
| --- | --- |
| 版本 | V3 |
| 序列号 | 0fa4bfef82e81e9c4e19bff2e5b9a087 |
| 签名算法 | sha256RSA |
| 签名哈希算法 | sha256 |
| 颁发者 | CN = GeoTrust CN RSA CA G1  OU = www.digicert.com  O = DigiCert Inc  C = US |
| 有效期从 | 2021年11月3日 8:00:00 |
| 到 | 2022年12月3日 7:59:59 |
| 使用者 | CN = \*.csdn.net  O = 北京创新乐知网络技术有限公司  S = 北京市  C = CN |
| 公钥 | RSA（2048 Bits）  30 82 01 0a 02 82 01 01 00 9a 79 10 da d8 87 06 98 63 bb 11 5a aa 4a 84 19 5b 2f 25 fe ea fe c6 de 23 b0 97 c2 3c 89 d7 53 0f 26 66 43 4f e2 cd 2f 23 57 6a 8c 8c fa 88 61 39 7e 96 9b 34 58 18 12 28 6d 48 64 b4 3b 6f 17 33 9f 1a e5 f4 7e 5b ae 11 81 72 e6 7d c6 b5 cf 8c 5f c8 b8 d5 ad 4e af 26 79 b4 39 9a 5e 6c 35 66 6b 65 27 8f fc 92 98 bc ec 3e 63 f9 8c 02 83 a0 5d 6d 2a bc c6 a0 5e 51 90 76 71 9c a9 9f 3a ce 87 60 b4 0d 09 cc f0 e5 7a b0 52 44 f7 19 f2 80 33 7a 8c ed 5b ba e6 95 8d 62 41 f5 b6 33 34 4a c0 95 b1 e5 bd 45 18 ba 00 30 46 88 0b 11 aa eb 12 52 fa 10 3f 89 f8 2b ba b9 92 07 76 75 73 08 fe f5 31 69 e6 43 f7 13 a0 9a d6 ef da 13 ae 5d ea 4b 49 3d dc 09 cc 23 16 d8 7d 83 20 31 0b 89 a9 7a 21 06 06 d3 20 ea 60 b8 75 b5 01 18 ec 33 5c c7 e1 ad 69 e8 8f 72 14 85 30 9d 19 93 0d 02 03 01 00 01 |
| 公钥参数 | 05 00 |
| 授权密钥标识符 | KeyID=919f5e3115ae109fad60c1f7c1ccaa48342f0c26 |
| 使用者密钥标识符 | 991632ab04abf867b9127ddf9da78da7cffc2cf2 |
| 使用者可选名称 | DNS Name=\*.csdn.net  DNS Name=csdn.net |
| 增强型密钥用法 | 服务器身份验证 (1.3.6.1.5.5.7.3.1)  客户端身份验证 (1.3.6.1.5.5.7.3.2) |
| CRL分发点 | [1]CRL Distribution Point  Distribution Point Name:  Full Name:  URL=http://crl3.digicert.com/GeoTrustCNRSACAG1.crl  [2]CRL Distribution Point  Distribution Point Name:  Full Name:  URL=http://crl4.digicert.com/GeoTrustCNRSACAG1.crl |
| 证书策略 | [1]Certificate Policy:  Policy Identifier=2.23.140.1.2.2  [1,1]Policy Qualifier Info:  Policy Qualifier Id=CPS  Qualifier:  http://www.digicert.com/CPS |
| 授权信息访问 | [1]Authority Info Access  Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1)  Alternative Name:  URL=http://ocsp.dcocsp.cn  [2]Authority Info Access  Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2)  Alternative Name:  URL=http://crl.digicert-cn.com/GeoTrustCNRSACAG1.crt |
| SCT列表 | v1  2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784  2021年11月3日 14:59:05  SHA256  ECDSA  3046022100be2dd8857d36484447f5ade50fe05d4188eec64661306378f225ed268a5606be022100c85ae7db5d224b96751df9e836494c3924739c205a5b968365e385c36d68d675  v1  51a3b0f5fd01799c566db837788f0ca47acc1b27cbf79e88429a0dfed48b05e5  2021年11月3日 14:59:05  SHA256  ECDSA  3045022100c02124ed87521cc37c500629ed8da8b21162631bb576c5e9ed43200c8aca1c9f022077f54d50550970b2d8792a2aa59143b99395d2e256569409571251b8aa379d24  v1  41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6  2021年11月3日 14:59:05  SHA256  ECDSA  3045022100b5d3a336f359048f9eb07fa42cf0fdba2155ae67433c49aca7e2b3280694e1bc0220666db2d3c9489afaa0dda18a796e889e5e174f06bc1c7e882f6f66584f534cc5 |
| 密钥用法 | Digital Signature, Key Encipherment (a0) |
| 基本约束 | Subject Type=End Entity  Path Length Constraint=None |
| 指纹 | 31c3e8e9aa426ce555abde8e117e716132ff36f2 |

## 公钥算法

RSA（2048bits）

公钥参数：05 00