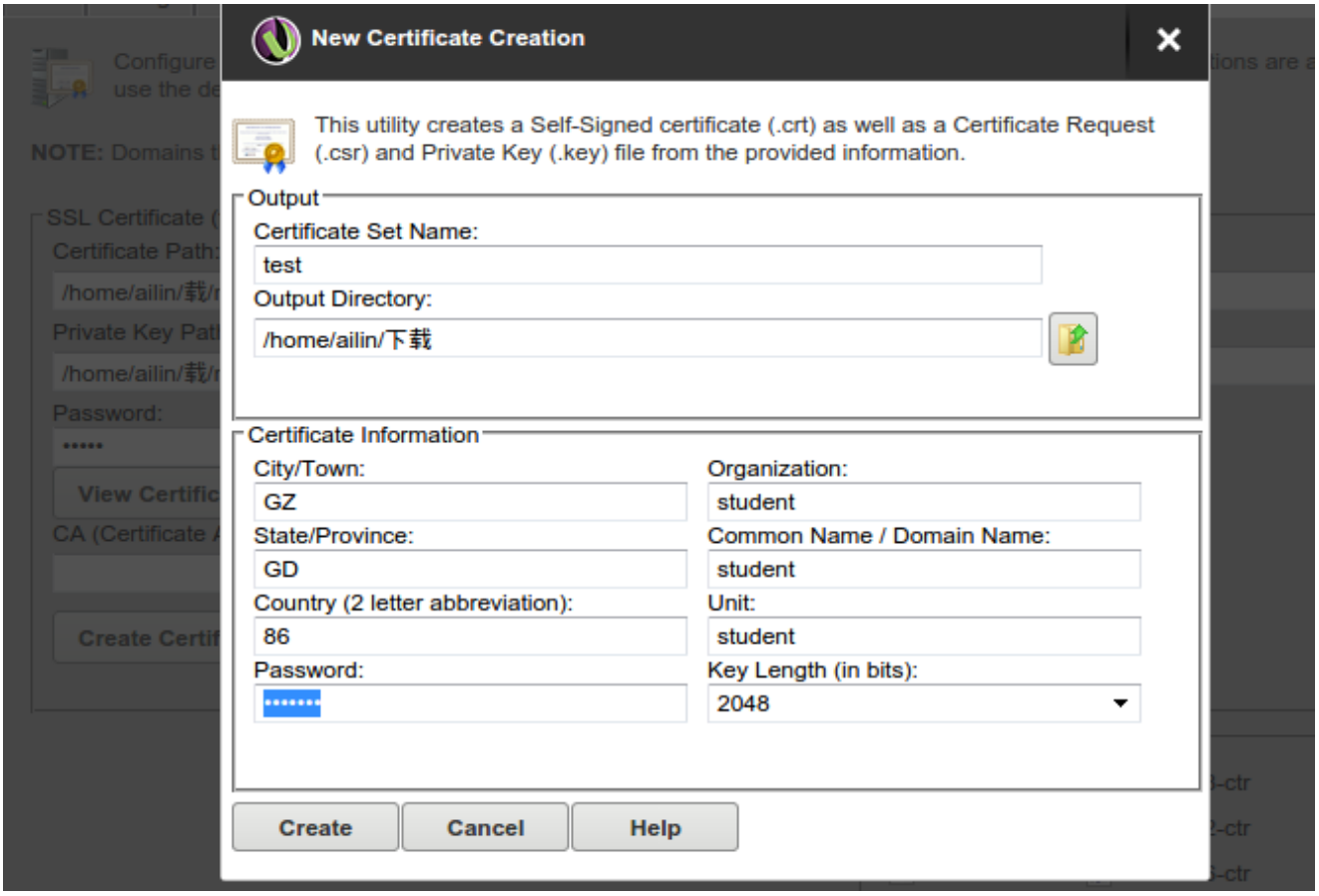
一个关于X.509的小例子和它的工作原理

因为前段时间做的计网实验里面有一部分涉及到了用SSL/TLS加密的ftp传输，这里面也是有x.509的证书有关知识在内，所以就以这个小例子来阐述X.509的工作过程了。

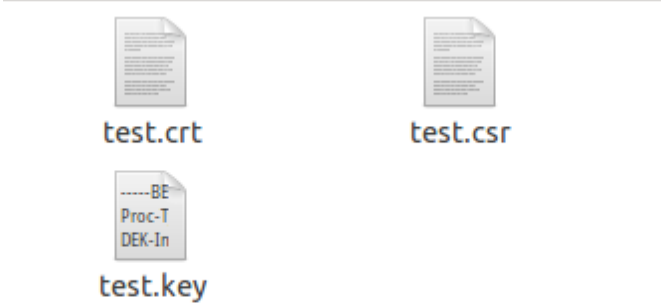
我是用的Serv-U在自己本机上面搭的一个ftp，其中当涉及到加密的部分的时候就会要求生成证书。

生成证书



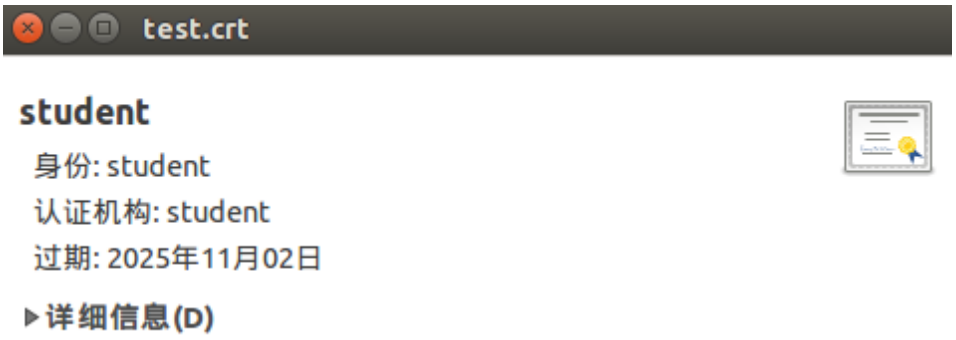
在里面填好相关信息还有密码以后，就会在本地生成证书还有公钥私钥

证书和公钥私钥导出



我们可以点开看看

CA证书里面的具体信息



颁发的证书

版本:	3
序列号:	00
在此之前无效:	2015-11-05
在此之后无效:	2025-11-02

证书指纹

SHA1:	17 99 80 93 DF B8 EB 61 A5 BB D3 B9 A3 89 E9 7B 4C D8 84 75
MD5:	9E A4 01 F5 B9 DA 1B 93 27 AE 29 2A E7 6C C1 C8

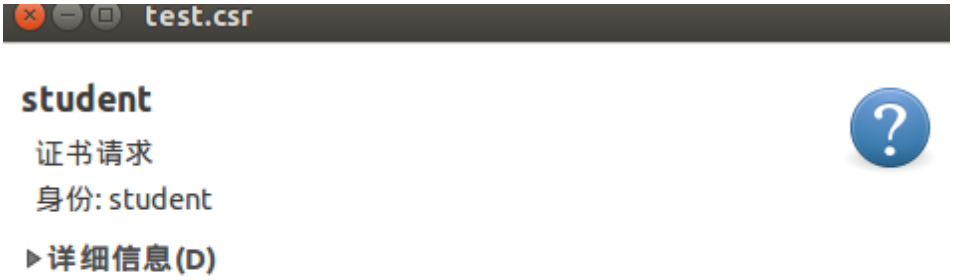
公开密钥信息

密钥算法:	RSA
密钥参数:	05 00
密钥大小:	2048
密钥 SHA1 指纹:	DD DA 95 00 E7 0E 5C 53 F3 4E 86 25 68 0A 60 5E 73 B7 B7 1E
公钥:	30 82 01 0A 02 82 01 01 00 BE EF 58 10 98 8E DF A3 6C D1 CA 04 39 E6 AF 05 AE FA F0 72 C0 BC 1C 94 13 FA 7C 19 D6 AA 40 6A 4A 22 AF C4 65 B3 64 18 84 56 5E 03 93 E8 77 06 E2 48 DD F5 F9 0A 8A CA 4F 6C 38 25 EB E4 11 1E 78 AB 83 7D 55 52 90 1B D8 C8 F4 F8 1F 6A 5F 36 5D E 8E C6 94 FA 49 42 B5 36 D6 1B C8 EA 4D 31 0F 8F 0D FB 95 52 D4 72 51 85 A4 F9 C7 C7 D7 DA AD 76 CF B8 8F 25 56 1E 98 83 74 8A 7E 60 57 E2 A7 FC 74 BE 84 A8 6C 8F AB FF 88 72 A9 91 4F C6 A2 B5 42 4A 1B F1 54 D9 58 09 75 67 31 E8 A0 CB BC 50 9F 13 27 18 16 70 BA AE C3 7F 3 B1 E1 43 86 2B F6 BE FF 8B CF 02 A6 C6 B9 3F 03 39 0C 40 AC 1A 88 A0 FD 3A B5 D2 23 16 F4 1F 15 3D F2 04 A3 DD 3D 0F A8 25 02 03 01 00 (

签名

签名算法:	使用 SHA1 算法的 RSA 密钥对
签名参数:	05 00
签名:	75 0D ED 91 4E 47 4A 04 0D E2 76 F3 9E E7 BA 15 92 D3 2D A0 C4 0B 1D 27 8D 18 8A 7C 97 4F 5F 4F 64 F9 F1 8A 9A 09 05 D3 BF 8D 80 F6 B8 02 C1 E8 A6 79 BA E8 62 6C 1A 47 DC CB 5B 33 80 56 88 BB CA C3 BA B0 15 81 7D 82 FB 8C 7C 9C 03 E6 4C CB 9D 74 54 A9 FC DF 36 09 70 8. 0F 8B 2B A6 E1 83 13 EF 6C 1E 03 F5 C1 3E 75 1C 12 38 08 95 3B B6 30 FD 03 D3 AB 6E A1 01 36 9C C3 DB 19 42 DD 26 6F 3A E2 7F F7 1C E9 A1 C0 46 4B 90 10 02 87 55 FD 19 19 AE 1C 25 60 B2 30 38 41 26 5A C7 DA 01 C3 81 62 44 FD EE E7 0D 52 23 66 DA 7F C5 EE 63 9D 46 F4 92 86 70 55 21 BC FD A9 34 B0 0B C5 20 38 C7 F8 27 5D 4B 92 B8 32 19 C8 4E 6D A3 69 F8 1F 98 F2 B5 F4

公钥里面的具体信息



证书请求

类型:	PKCS#10
版本:	1

公开密钥信息

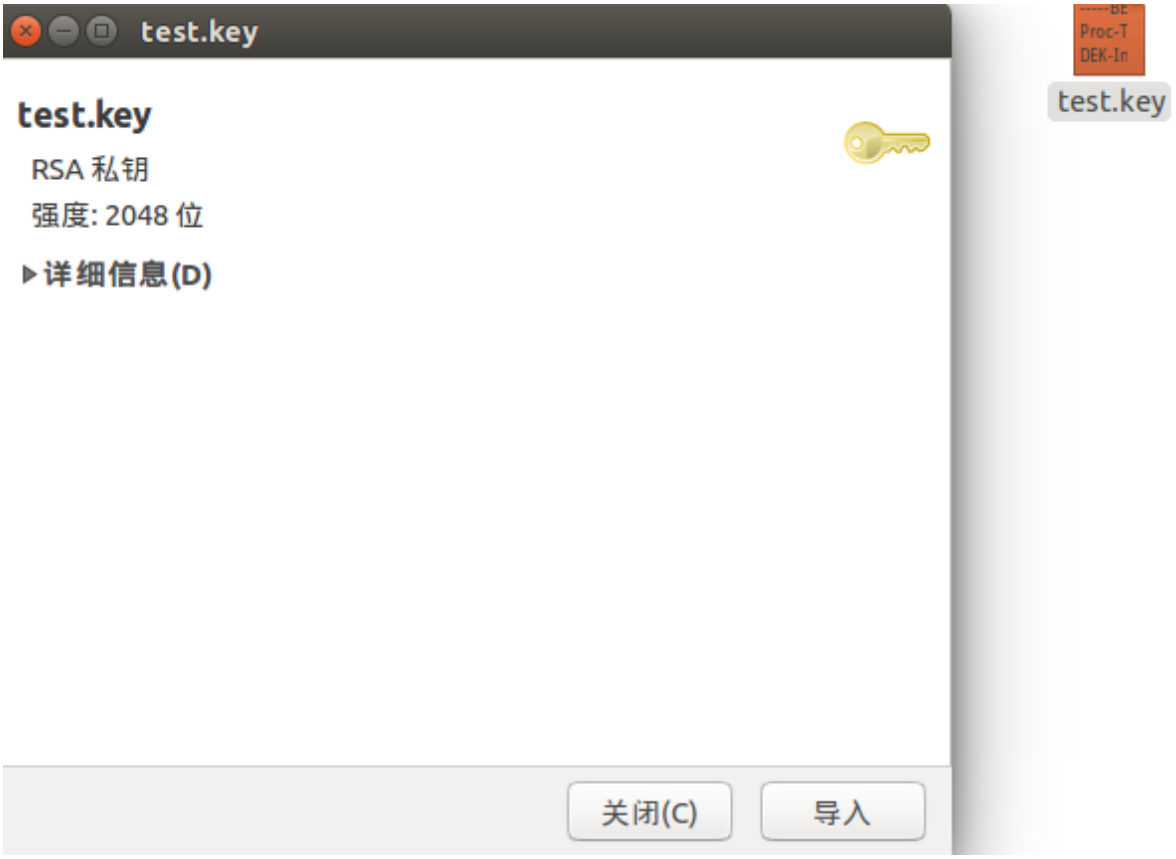
密钥算法:	RSA
密钥参数:	05 00
密钥大小:	2048
密钥 SHA1 指纹:	DD DA 95 00 E7 0E 5C 53 F3 4E 86 25 68 0A 60 5E 73 B7 B7 1E
公钥:	30 82 01 0A 02 82 01 01 00 BE EF 58 10 98 8E DF A3 6C D1 CA 04 39 E6 AF 05 AE FA F0 72 C0 BC 1C 94 13 FA 7C 19 D6 AA 40 6A 4A 22 AF C4 E1 E6 FF 3A DE C6 87 C8 4E 3F 84 65 B3 64 18 84 56 5E 03 93 E8 77 06 E2 48 DD F5 F9 0A 8A CA 4F 6C 38 25 EB E4 11 1E 78 AB 83 7D 55 52 90 1B D8 C8 F4 F8 1F 6A 5F 36 5D BB CB BD 24 0C 57 6A 07 79 81 63 8E C6 94 FA 49 42 B5 36 D6 1B C8 EA 4D 31 0F 8F 0D FB 95 52 D4 72 51 85 A4 F9 C7 C7 D7 DA AD 76 CF B8 8F 25 56 1E 98 83 74 8A 7E 60 57 E3 FF 6F 09 D4 C5 12 24 14 90 28 E2 A7 FC 74 BE 84 A8 6C 8F AB FF 88 72 A9 91 4F C6 A2 B5 42 4A 1B F1 54 D9 58 09 75 67 31 E8 A0 CB BC 50 9F 13 27 18 16 70 BA AE C3 7F 38 59 CA B8 B8 0A 59 3B 39 9D A0 B1 E1 43 86 2B F6 BE FF 8B CF 02 A6 C6 B9 3F 03 39 0C 40 AC 1A 88 A0 FD 3A B5 D2 23 16 F4 1F 15 3D F2 04 A3 DD 3D 0F A8 25 02 03 01 00 01

签名

签名算法:	使用 SHA1 算法的 RSA 密钥对
签名参数:	05 00
签名:	10 A2 42 EA 5C 6A 7D 25 9A A4 CE 0F 87 6A DE A3 A9 F8 19 AA BA 27 A4 21 B6 7C 88 BB A2 9D 32 95 BB 99 B0 1A 40 73 AC B2 B2 9C 55 AB 94 74 FE B2 3B 7E EF 1C F6 6B 01 9A CF F1 19 97 58 97 BC 09 46 B7 95 17 34 59 70 8F 8F B6 CD AF 3C CE F2 BC A8 3C 83 58 51 26 A7 54 78 D9 35 86 1F 3D D3 29 A6 BF 70 CD 84 38 AE 1B 66 C9 30 87 28 C9 D7 BF F4 E7 47 52 AA 2A 93 2F C0 AB 86 3A D0 2B CC 0E 7A C6 8C C3 A8 8C CB B0 74 AF 01 46 A9 A2 39 26 41 3D EA DA 3D CA CF 6A 88 0C 37 CA 57 CE DF 70 0B 0B 37 37 3D 36 A5 E1 97 F1 32 37 55 EE E6 A5 42 9F E8 4C 05 14 EA 48 56 8E 6E 56 22 9E EC 20 97 9F 26 6E F4 BB 6B F9 63 61 21 8D DF F8 B6 BD EB 10 54 AE BC 5E 43 82 A4 6E F6 00 A8 EF B8 69 37 0A E3 90 FE 6E CC B9 1C 88 A0 A5 16 74 9C E2 93 98 4A 18 A2 62 03 8F D9 50 40 37 6F ED F4 DC

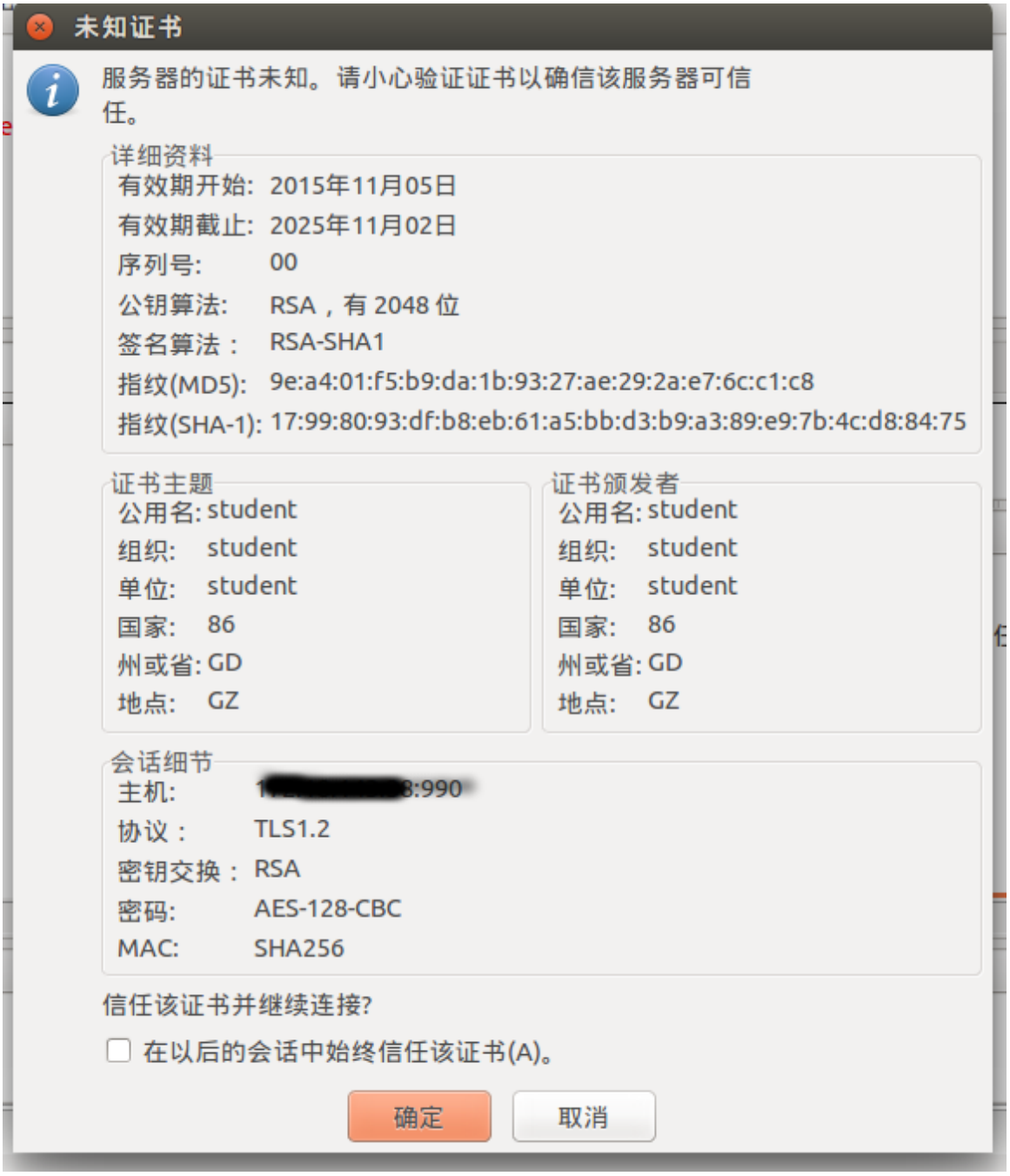
私钥里面的具体信息

（这是要输入了我们开始设置的密码才可以显示出来的）



当客户端来连接服务器

客户端会显示这个消息（因为我们自己生成的这个证书是没有真正去授权的）



客户端一方选择确定以后就可以正常登陆到ftp上进行操作了。

工作流程

这里的公钥私钥应该只会在握手阶段的时候用上。

我们先要弄清楚的一点是：只有公钥才能解密经私钥加密的内容，只有私钥才能解密经公钥加密的内容。

1. 客户端访问服务器的时候，服务器先发送一个带有公钥在内的证书给客户端。
2. 客户端验证服务器发过来的证书，如果发现证书有问题的话，就会提示用户（就是刚刚弹出来的框框）
3. 然后我们刚刚选择了信任该证书，因此客户端就从证书中取出了公钥，然后客户端生成一个随机数k，利用公钥加密，得到的密文发回给服务器。
4. 只有服务器拥有私钥，所以之后服务器才能解密，看到随机数k，这个时候服务器还有客

户端都知道了k，在之后的通信中用k进行加密通信