GSSAPI _SSLEAY for Globus Security

Douglas E. Engert

DEEngert@anl.gov

Argonne National Laboratory

03/20/1998

COPYRIGHT STATUS: Documents authored by Argonne National Laboratory employees are the result of work under U.S. Government contract W-31-109-ENG-38 and are therefore subject to the following license: The Government is granted for itself and others acting on its behalf a paid-up, nonexclusive, irrevocable worldwide license in these documents to reproduce, prepare derivative works, and perform publicly and display publicly by or on behalf of the Government.

Introduction

- The Globus Project
- SSLeay
- GSSAPI_SSLEAY
- The bigger picture
- Local Authentication to Kerberos V5
- Futures

GLOBUS Project

- Enable the construction of networked virtual computers
- Authentication
  - Gram_client
  - Gatekeeper
    - » Controlled by local site
- A user has a globusid, and local accounts/username etc.
- Mutual authentication

SSLeay

- SSLeay -0.8.1
- Eric A. Young - Australia
- SSLv3
  - Mutual Authentication
  - X509
  - Encrypted streams
  - Multiple hashes, encryption, authentication

GSSAPI_SSLEAY

- GSSAPI for security
- IETF Draft C bindings
  - "Generic Security Service API Version 2 : C-bindings", John Wray, 11/24/1997.
- Partially implementation of draft
  - No gss_wrap, gss_unwrap

X509_USER_KEY


```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,50E478A89A4D3CAB

QgPYlNdJGqk6zzyGKVKasdfjlsdfDZ:LJrsgfjsonmzEZvFvzO9KjzlHLxu9w3vH
yBf5h3FPSVI4D3dX4JaPirVocMFJfbsQNn7pbJ65xBDJs86FCTd6nXI0dZfs7Xu9
mJL2dY+pc4Aq9msDPaotfEewnBHlk42qk44v29A1gPkpdIi+R58192rGwUAzMxHN
J1VvNBNKtdpfmaHEgWTjodauOBofXwq7tARytBqEf3WinA3FYLQ9ob3J4VTm5Tsq
6PDjdMOHH6lLz3qh9QRRGPRMH+VYAicKPCJ96RIB7YU3aVjzqr0ebJ6Ux1O7yDQv
RUmMHfN5TJ3pPjppnothisisnotmyreallkeyWTRvkcvfQc3/0OBXfhQZRp/FHDw
bjZs/FPP7JgVtuF4L2IvbQcrrSt7CKySXeGO2FAa/GbBfI3WUIy5eMOzumpCTza+
qY9B1kkfbio8V63Iwmd56zgOtl2wvTxMzVXxbLMZ9ybF5rX3x1eXnsZ0BBaxMieD
ND71GQR50oBJ/HTxheNBYIhavechangedmanyofthecharactersULMR6iMnt2AO
O1XzV2riQqePjj4zZFLuZ/wSkGcpNk+ZIZ2qbMxQiUjt0EfvqdtH4PTAQUSfcGBp
5gCTUcXJBG2t3Mc32Ivc4ipUj1Ivv6oHsMLFES6jjLtglvSDbGcAKhToO4Cc2pon
wiGCFSviPWjXR+FJWuxP8igoxLmjA16+qFrB7Z4GAXF5tsV2+l0inl/ItW07J+yk
WvI6Vv5y9NI9GEPH3ZPY9L6jyIU0TCj2jbg2fa62pBej2TfNphphsw==
-----END RSA PRIVATE KEY-----
```

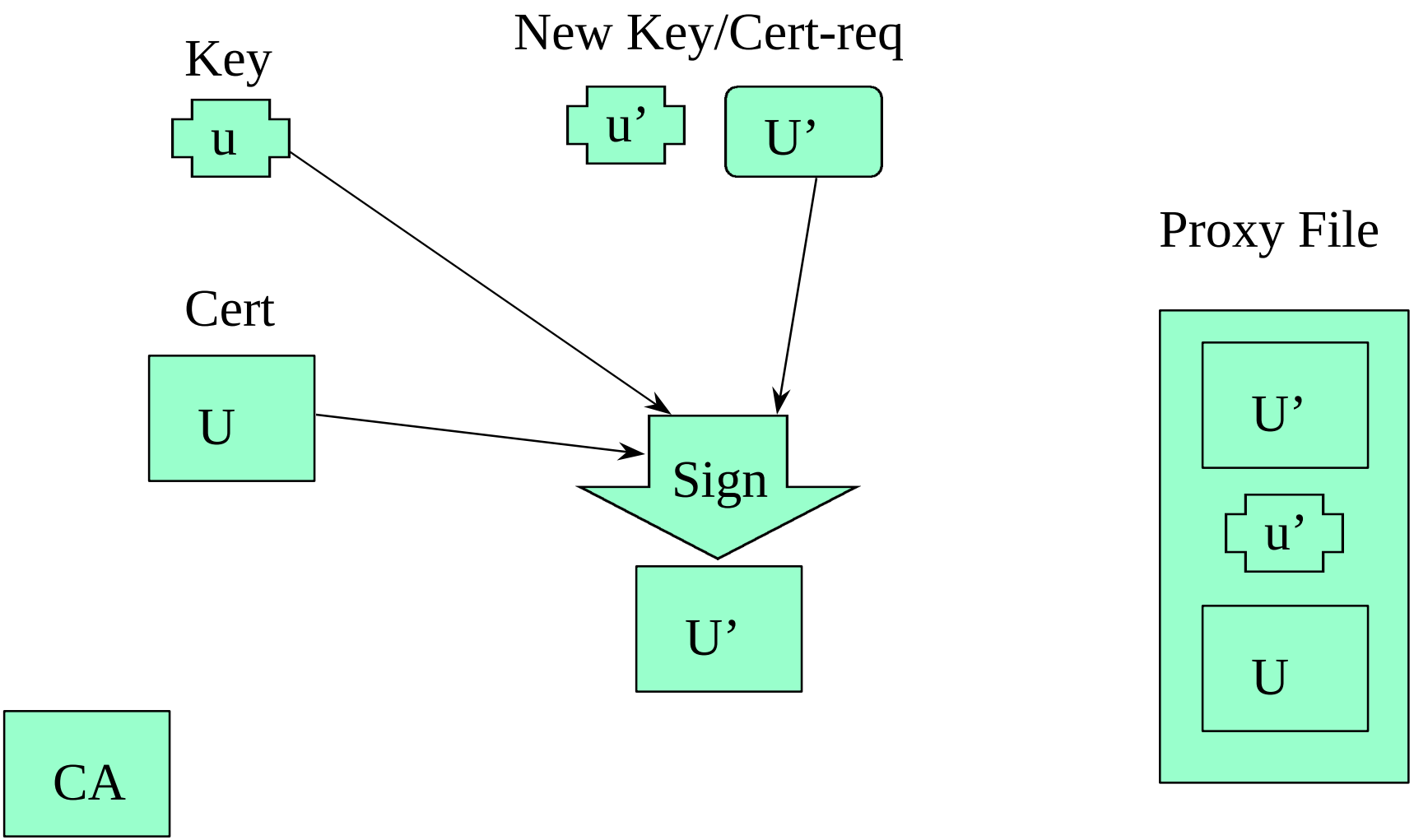
X509_USER_CERT


```
-----BEGIN CERTIFICATE-----
MIICAjCCAWugAwIBAgIBATANBgkqhkiG9w0BAQQFADBHMQswCQYDVQQGEwJVUzEP
MA0GA1UEChMGR2xvYnVzMScwJQYDVQQDEx5HbG9idXMgQ2VydGlmaWNhdGlvbiBB
dXRob3JpdHkwHhcNOTgwMTIzMjAxODExWhcNOTkwMTIzMjAxODExWjAwMQswCQYD
VQQGEwJVUzEPMA0GA1UEChMGR2xvYnVzMRAwDgYDVQQDEwdkZW5nZXJ0MIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQDGlHKbsLtNNww3W5xztmzfDlw4Dl3tGruN
3ahpa1zF/I/57BB9nPUFG8i9MuDpKG4uziYrz0s8D3O1Zuax3aINCih2KuiMWobI
DqauqYuWisq7wDuS3U153QiVd3d/4S2wx71II7k+TifWq3L4NHvWangPGNYGYt0w
EY+8PKqJjQIDAQABoxUwEzARBglghkgBhvhCAQEEBAMCAEAwDQYJKoZIhvcNAQEE
BQADgYEAlCEkFmEu+l5l3UaNIijJY9Re2wTM3urL2M+Sdpil6MMISwOVtufy7HPb
E9zT6CrGI1trDTtBhRRPlzS9DoLn/J05/Ya0chxIyHKX1Nlpy57dyaJbnscQf6of
vf3NkoEERDVMR5o0/32AMsRYWASFtJBJovmgJnYZ9yd8Bjl9Ho0=
-----END CERTIFICATE-----
```

Readable User Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, O=Globus, CN=Globus Certification Authority
        Validity
            Not Before: Jan 23 20:18:11 1998 GMT
            Not After : Jan 23 20:18:11 1999 GMT
        Subject: C=US, O=Globus, CN=dengert
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c6:94:72:9b:b0:bb:4d:37:0c:37:5b:9c:73:b6:
                    6c:df:0e:5c:38:0e:5d:ed:1a:bb:8d:dd:a8:69:6b:
                    5c:c5:fc:8f:f9:ec:10:7d:9c:f5:05:1b:c8:bd:32:
                    e0:e9:28:6e:2e:ce:26:2b:cf:4b:3c:0f:73:b5:66:
                    e6:b1:dd:a2:0d:0a:28:76:2a:e8:8c:5a:86:c8:0e:
                    a6:ae:a9:8b:96:8a:ca:bb:c0:3b:92:dd:4d:79:dd:
                    08:95:77:77:7f:e1:2d:b0:c7:bd:48:23:b9:3e:4e:
                    27:d6:ab:72:f8:34:7b:d6:6a:78:0f:18:d6:06:62:
                    dd:30:11:8f:bc:3c:aa:89:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Netscape Cert Type:
                ...@
    Signature Algorithm: md5WithRSAEncryption
        94:21:24:16:61:2e:fa:5e:65:dd:46:8d:22:28:c9:63:d4:5e:
        db:04:cc:de:ea:cb:d8:cf:92:76:98:a5:e8:c3:08:4b:03:95:
        b6:e7:f2:ec:73:db:13:dc:d3:e8:2a:c6:23:5b:6b:0d:3b:41:
        85:14:4f:97:34:bd:0e:82:e7:fc:9d:39:fd:86:b4:72:1c:48:
        c8:72:97:d4:d9:69:cb:9e:dd:c9:a2:5b:9e:c7:10:7f:aa:1f:
        bd:fd:cd:92:81:04:44:35:4c:47:9a:34:ff:7d:80:32:c4:58:
        58:04:85:b4:90:49:a2:f9:a0:26:76:19:f7:27:7c:06:39:7d:
        1e:8d
```

cinit Program



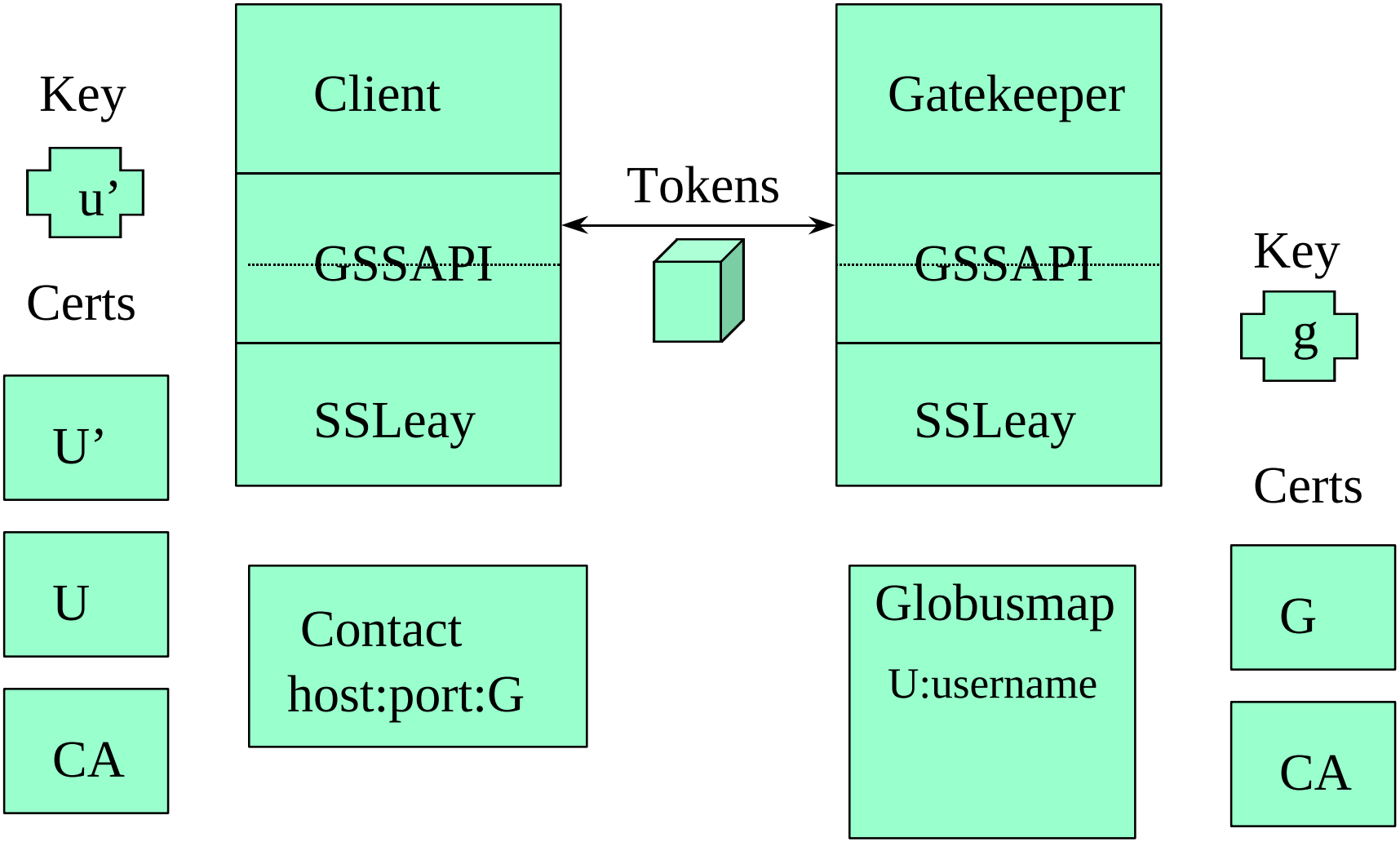
X509_USER_PROXY


```
-----BEGIN CERTIFICATE-----
MIIBtTCCAR6gAwIBAgIBATANBgkqhkiG9w0BAQQFADAwMQswCQYDVQQGEwJVUzEP
MA0GA1UEChMGR2xvYnVzMRAwDgYDVQQDEwdkZW5nZXJ0MB4XDTk4MDMxNjE5MzMx
NFoXDTk4MDMxNzAzMzMxNFowPjELMAkGA1UEBhMCVVMxDzANBgNVBAoTBkdsb2J1
czEeMA4GA1UEAxMHZGVuZ2VydDAMBgNVBAMTBXByb3h5MFwwDQYJKoZIhvcNAQEB
BQADSwAwSAJBAMvW9fPaBYDf0ziBPyqujqzN7qg/prU2bW+Fhye3/uDFV/iOhxuI
XgedXpGBAXIAyM1idextX6vCqvbsCNHsi7kCAwEAAaMVMBMwEQYJYIZIAYb4QgEB
BAQDAgBAMA0GCSqGSIb3DQEBBAUAA4GBADW3I6uusMxAxC6hWA3KwKl+koCRwqOU
5zKiAduZ+mNmekqZmPskZTaca62NEJgdg/nODMoraOqKRDfiw8uIlTUhC+h1jW8P
tBz1KZWosE2Z3zvpQ3aqWnGzT4X19HccJYexb5dvExjdC3BKbNMnN2NL08+ugQp1
qTgCI/jUBI1V
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAMvW9fPaBYDf0ziBPyqujqzN7qg/prU2bW+Fhye3/uDFV/iOhxuI
XgedXpGBAXIAyM1idextX6vCqvbsCNHsi7kCAwEAAQJAQIxMjDChB4NZLo53AzwN
gBkiFvM5Bi87DlKZTvGL637hMD9C6a2WJuYTf67DS54E2Q26P+pCpjn75hhexzF3
ZQIhAPnSRDeXnMnWe6wfn5GTgcLXve/d0MxnZchkD2JvBLDTAiEA0OGQM7MJMtu6
zRrf6Fu17FNJhTwpG366F06nvohN2cMCIQDfzhd/FjxINfYlhU8Ww+cD/vMR6M4d
0KPGmp2NuZeiMQIgZriWdqYz/tvJ6HWv6Q+4zmhC/o+QU6Ill7KpkWxshIsCIQDr
H9xs4yReRjcGQFioj7fS0MmVQcEZ7Z1oUPt9EEwzEg==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICAjCCAWugAwIBAgIBATANBgkqhkiG9w0BAQQFADBHMQswCQYDVQQGEwJVUzEP
MA0GA1UEChMGR2xvYnVzMScwJQYDVQQDEx5HbG9idXMgQ2VydGlmaWNhdGlvbiBB
dXRob3JpdHkwHhcNOTgwMTIzMjAxODExWhcNOTkwMTIzMjAxODExWjAwMQswCQYD
VQQGEwJVUzEPMA0GA1UEChMGR2xvYnVzMRAwDgYDVQQDEwdkZW5nZXJ0MIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQDGlHKbsLtNNww3W5xztmzfDlw4Dl3tGruN
3ahpa1zF/I/57BB9nPUFG8i9MuDpKG4uziYrz0s8D3O1Zuax3aINCih2KuiMWobI
DqauqYuWisq7wDuS3U153QiVd3d/4S2wx71II7k+TifWq3L4NHvWangPGNYGYt0w
EY+8PKqJjQIDAQABoxUwEzARBglghkgBhvhCAQEEBAMCAEAwDQYJKoZIhvcNAQEE
BQADgYEAlCEkFmEu+l5l3UaNIijJY9Re2wTM3urL2M+Sdpil6MMISwOVtufy7HPb
E9zT6CrGI1trDTtBhRRPlzS9DoLn/J05/Ya0chxIyHKX1Nlpy57dyaJbnscQf6of
vf3NkoEERDVMR5o0/32AMsRYWASFtJBJovmgJnYZ9yd8Bjl9Ho0=
-----END CERTIFICATE-----
```

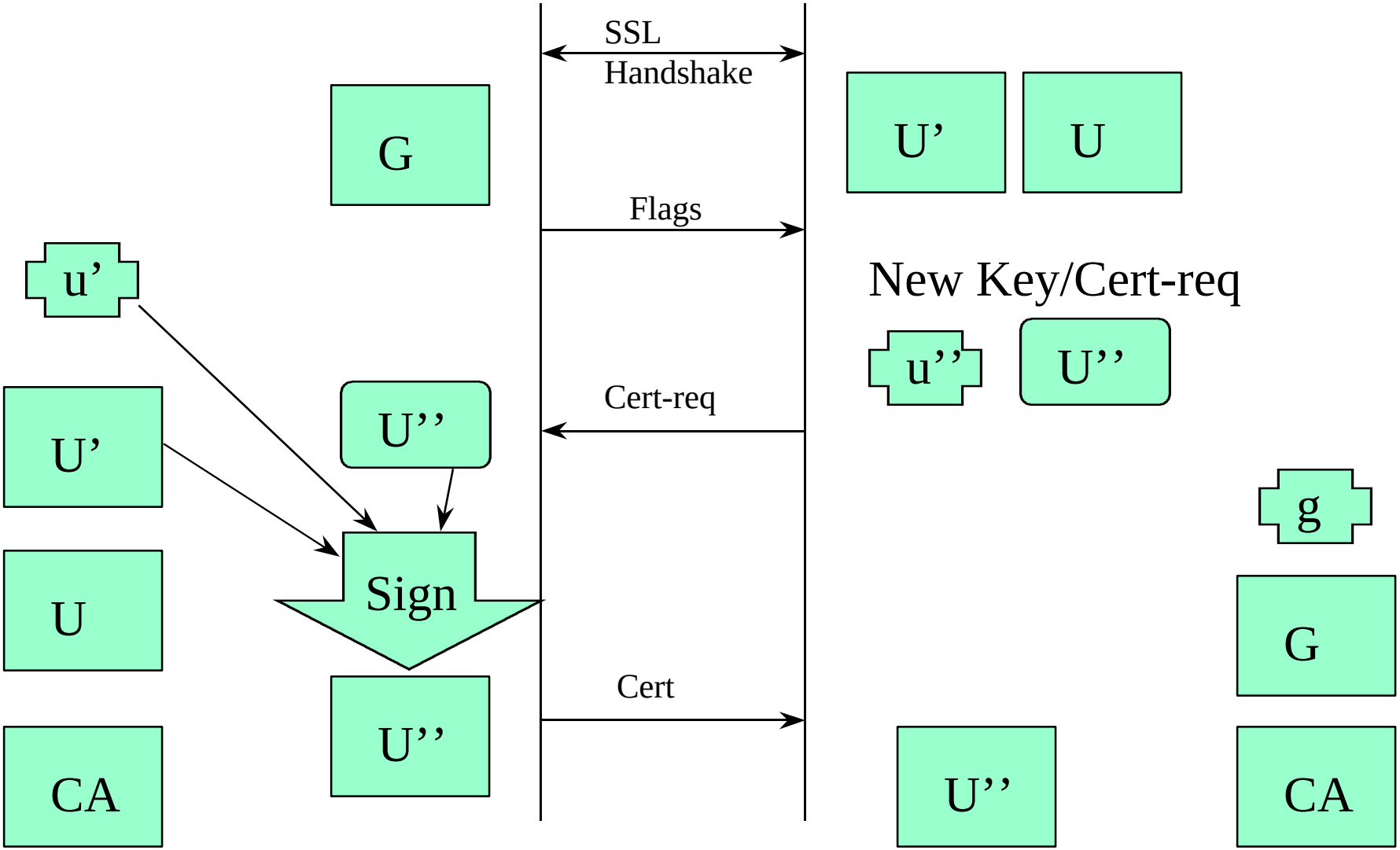
Proxy Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, O=Globus, CN=dengert
        Validity
            Not Before: Mar 16 19:33:14 1998 GMT
            Not After : Mar 17 03:33:14 1998 GMT
        Subject: C=US, O=Globus, CN=dengert, CN=proxy
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00:cb:d6:f5:f3:da:05:80:df:d3:38:81:3f:2a:ae:
                    8e:ac:cd:ee:a8:3f:a6:b5:36:6d:6f:85:87:27:b7:
                    fe:e0:c5:57:f8:8e:87:1b:88:5e:07:9d:5e:91:81:
                    01:72:00:c8:cd:62:75:ec:6d:5f:ab:c2:aa:f6:ec:
                    08:d1:ec:8b:b9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Netscape Cert Type:
                ...@
    Signature Algorithm: md5WithRSAEncryption
        35:b7:23:ab:ae:b0:cc:40:c4:2e:a1:58:0d:ca:c0:a9:7e:92:
        80:91:c2:a3:94:e7:32:a2:01:db:99:fa:63:66:7a:4a:99:98:
        fb:24:65:36:9c:6b:ad:8d:10:98:1d:83:f9:ce:0c:ca:2b:68:
        ea:8a:44:37:e2:c3:cb:88:95:35:21:0b:e8:75:8d:6f:0f:b4:
        1c:f5:29:95:a8:b0:4d:99:df:3b:e9:43:76:aa:5a:71:b3:4f:
        85:f5:f4:77:1c:25:87:b1:6f:97:6f:13:18:dd:0b:70:4a:6c:
        d3:27:37:63:4b:d3:cf:ae:81:0a:75:a9:38:02:23:f8:d4:04:
        8d:55
```

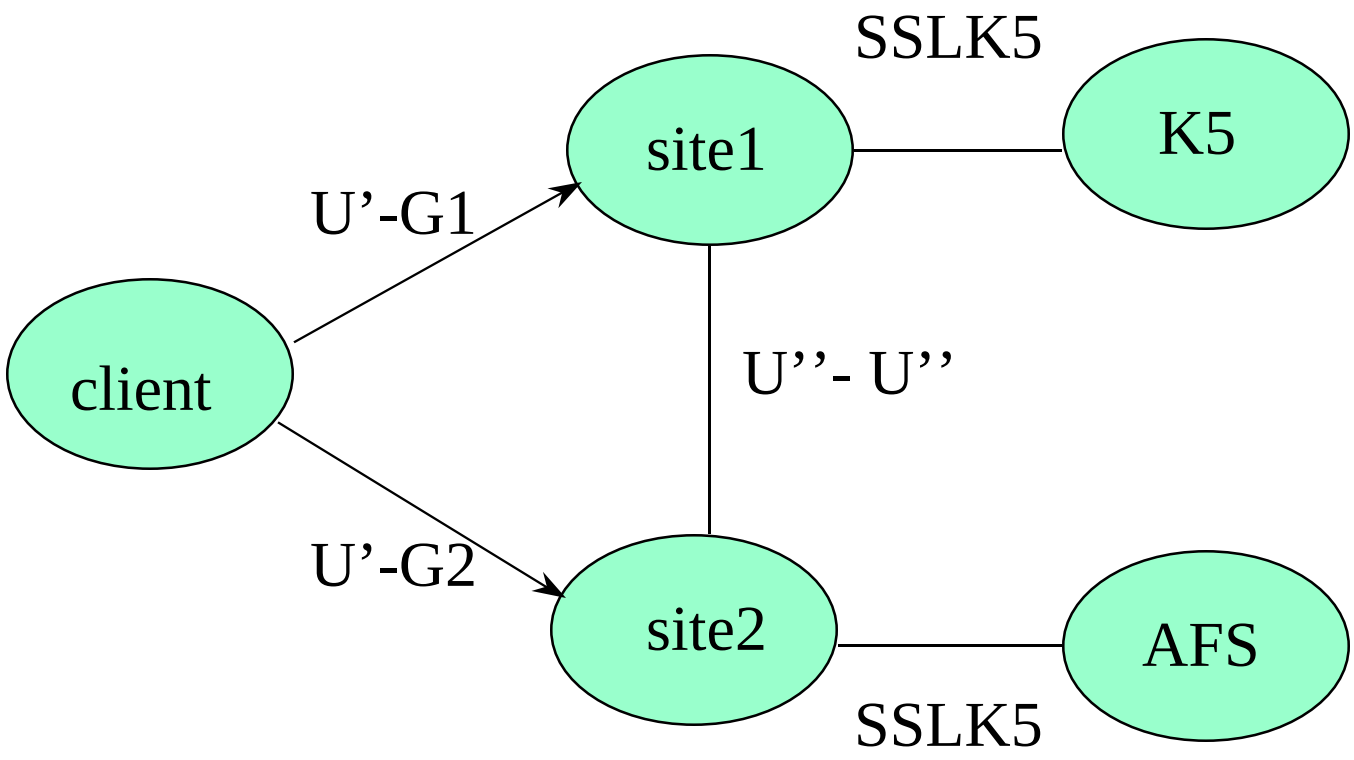
GSSAPI_SSLEAY - Proxy



GSSAPI_SSLEAY-proxy

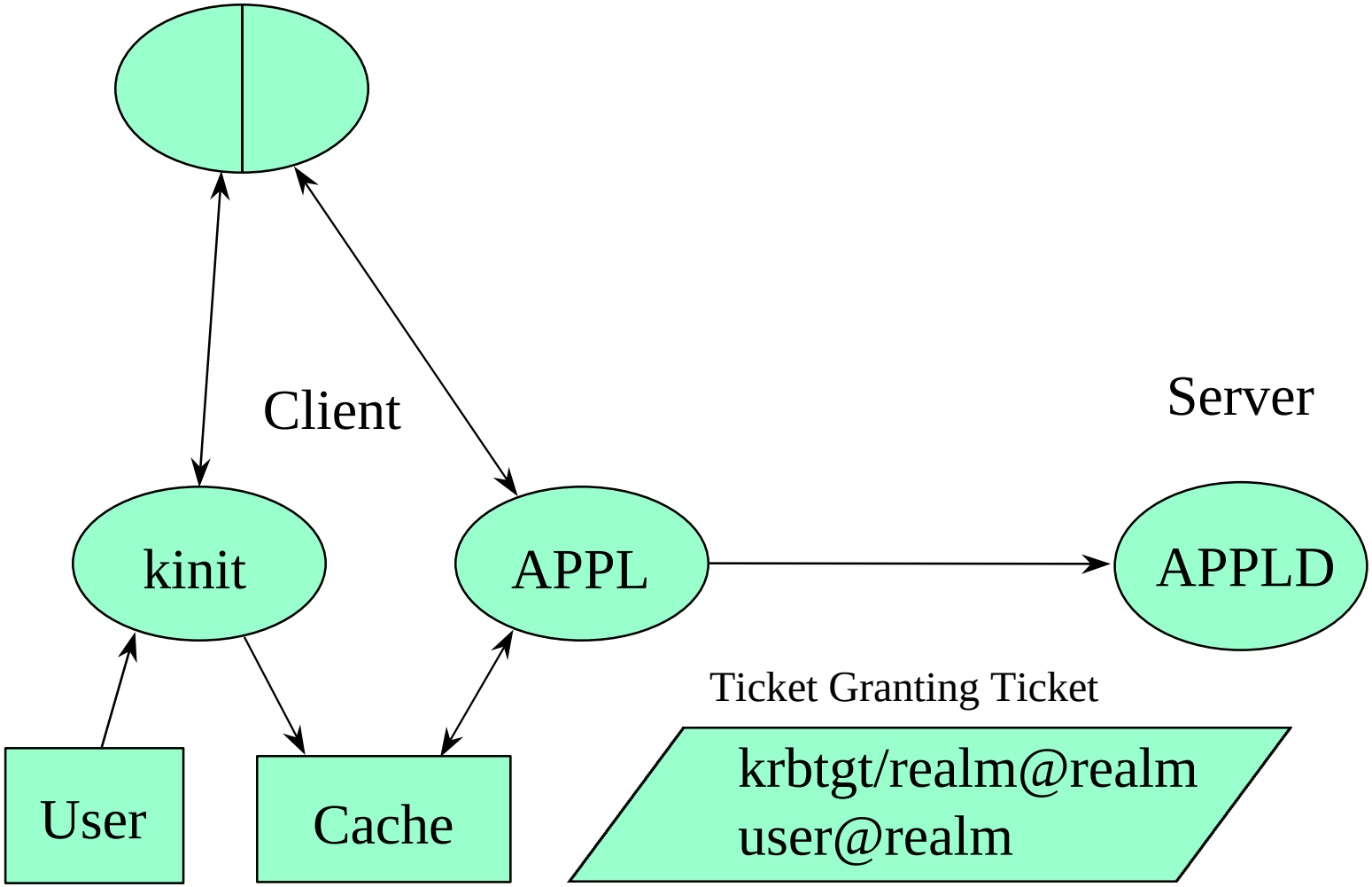


Local Site Authentication

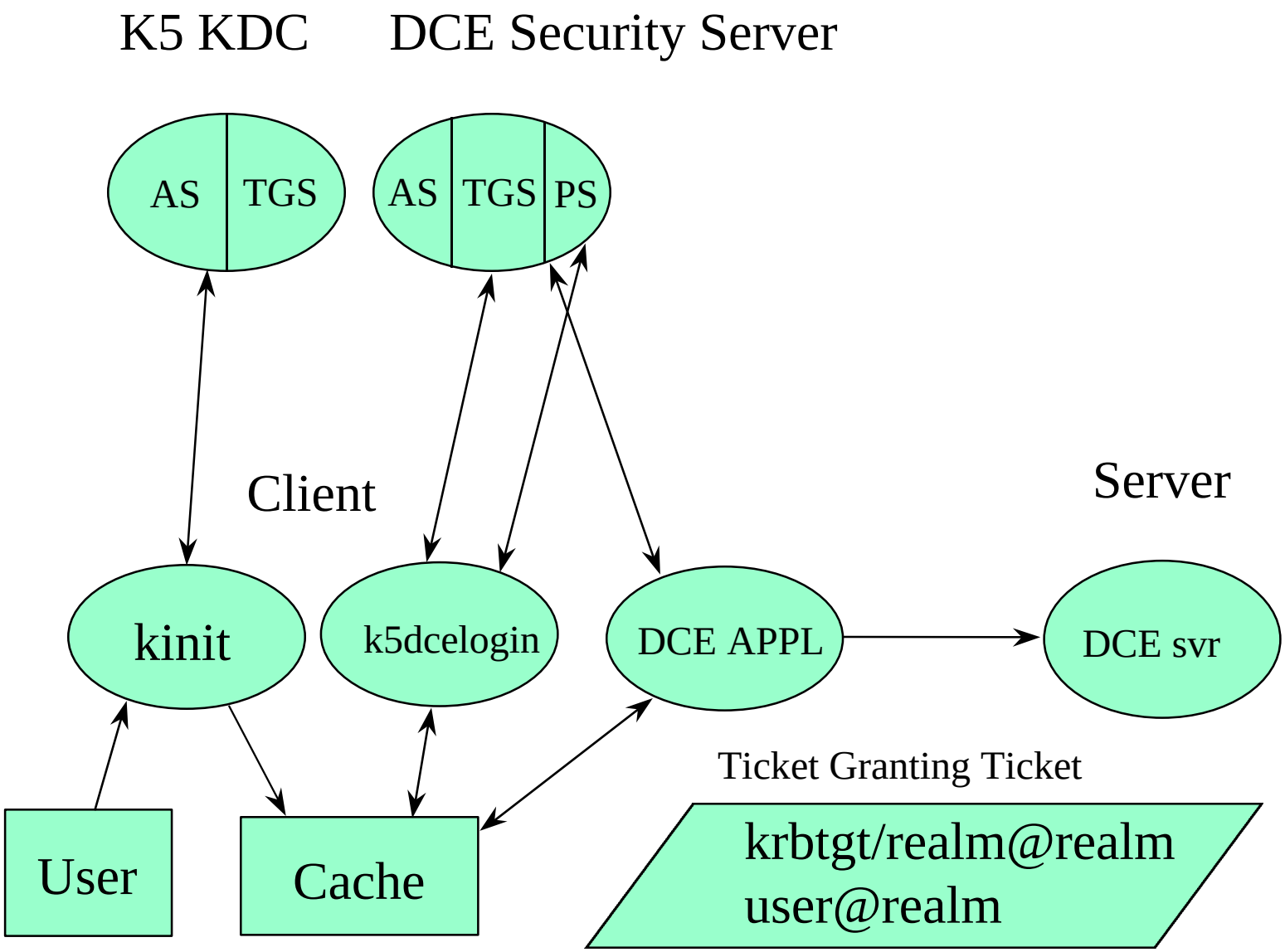


Kerberos Basics

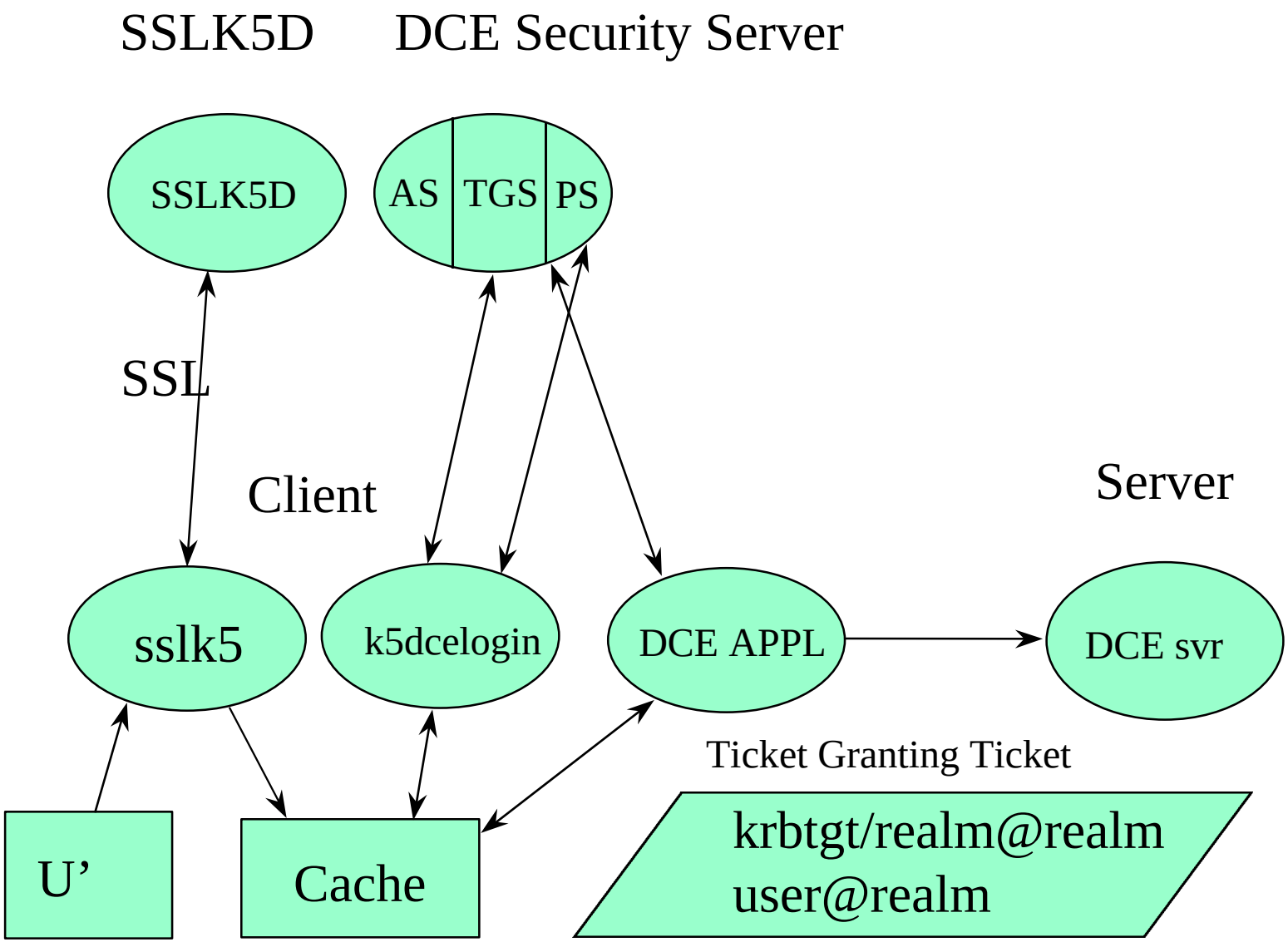
Key Distribution Center KDC or DCE Security Server



K5 KDC with DCE



SSL to Get K5 TGT



Futures

- X509 extensions
- limit proxy levels
- Limit usability
- Multiple CA
- Better Certificate chain processing
- Browser usage?
- CRLs

The End