Security in a Computational Grid Environment

Douglas E. Engert

DEEngert@anl.gov

Argonne National Laboratory

10/2000

Introduction

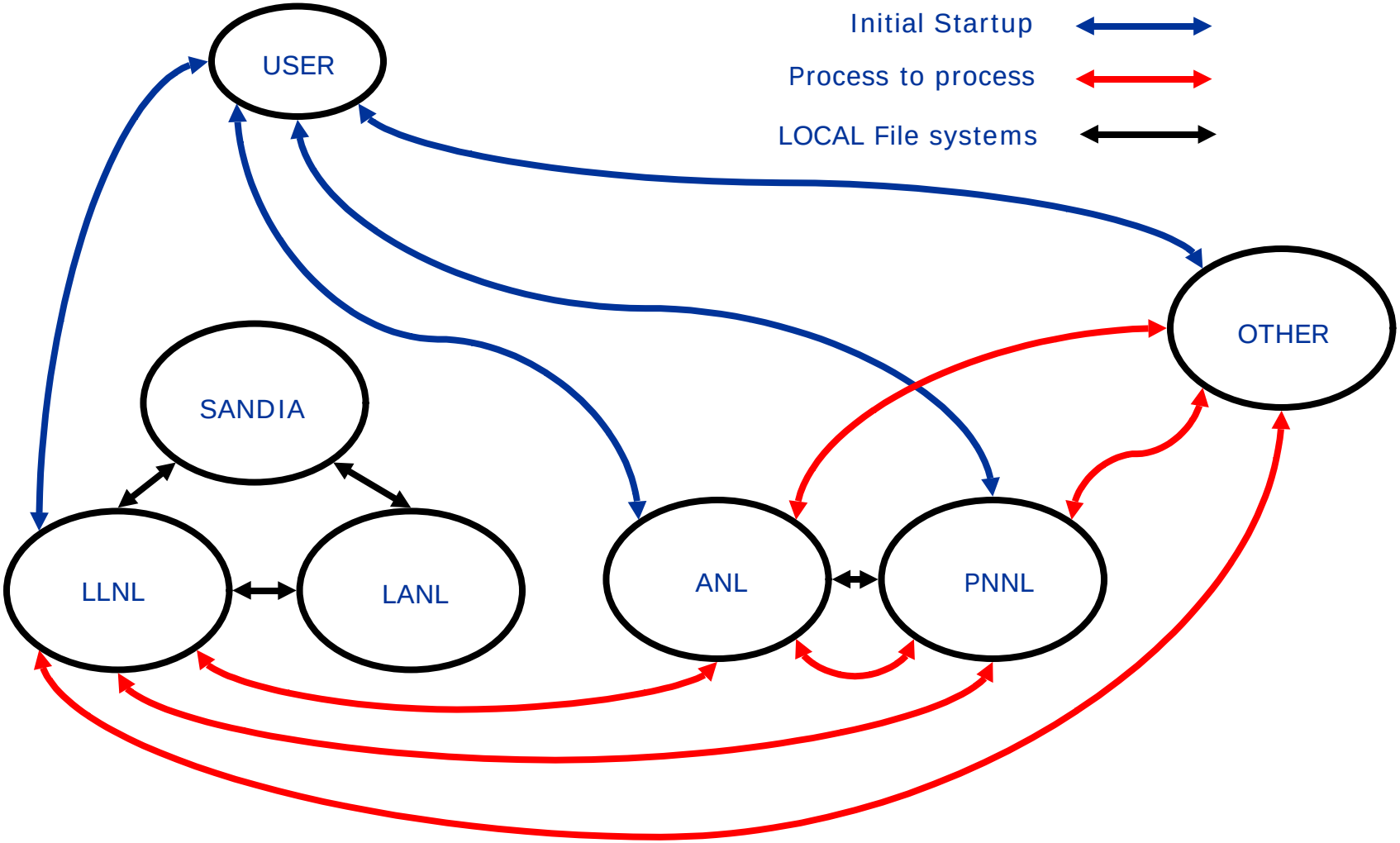
- The GRID Environment
- Security issues for the GRID Environment
- Its more then Client - Server!
- Globus GSI
- GSSAPI
- Delegation - Proxy Certificates
- Interfacing to local site security
- GSI vs. Kerberos
- Conclusions

The GRID Environment

- Multiple supercomputers
  - Each may have own job scheduler
- Multiple organizations
  - DOE, DoD, NASA, NSF, Universities
- User has accounts on each
  - Local control of resources
- User runs a job across the GRID creating a virtual supercomputer

the globus project
www.globus.org

A GRID Virtual Supercomputer



Security Issues for GRID Environment

- Multiple Organizations
  - May not have MOUs, but user has accounts
- Process to process communication
  - User's processes act as servers to other processes
  - Need authentication at least
  - Firewall issues
- May need credentials for local resources such as DFS or AFS

Its More then Client - Server!

- Processes start other processes
- Processes act as servers
- Process to process authentication, integrity, encryption
- Local control of resources
- Local security infrastructures

Globus

- Enables the construction of networked virtual supercomputers
  - http:\\www.globus.org
- Multiple Components - A toolkit
  - Scheduling, I/O, Naming Services ...
- Security Component - GSI
  - Globus/Grid Security Infrastructure
  - Single sign-on

Globus/Grid Security Infrastructure

- Globus Security adopted by Grid Forum and renamed to Grid Security Infrastructure
  - Widely adapted: DOE, DoD, NCSA, NPACI, NASA, among others
  - Installations on five continents
  - Globus CA in operation since 1998

GSI Features

- Public key certificates X.509 (standard)
  - Multiple CAs
  - Commercial CAs
- SSLv3 protocol (standard)
  - SSLeay or OpenSSL
- Delegation
  - “Proxy” certificates - short term
- U. S. export exemption
  - We also have encryption if you need it
- GSSAPI implementation (standard)

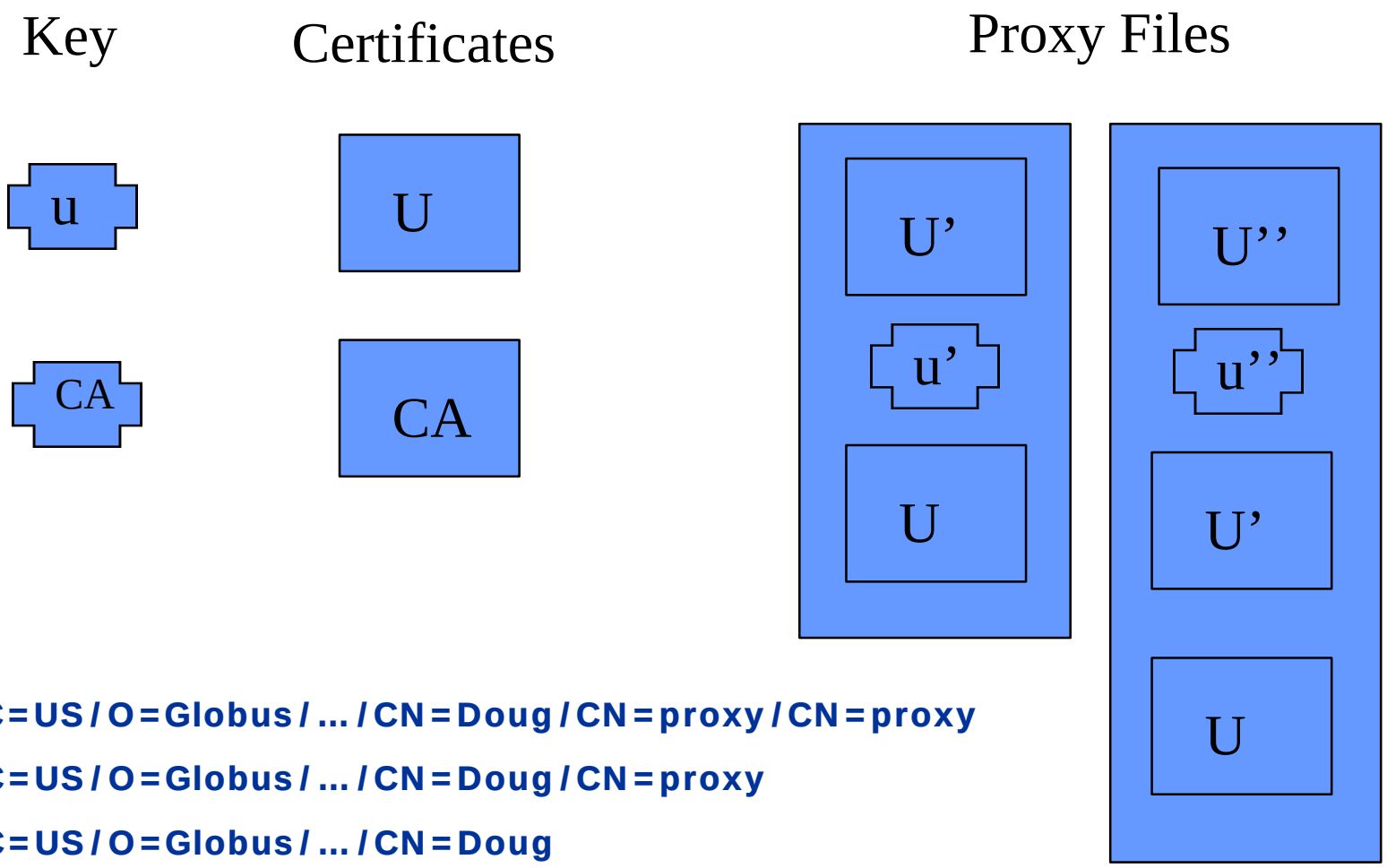
GSI Applications

- Globus
- SSH mods for GSSAPI authentication
  - ssh-1.2.27
  - SecureCRT
    - Commercial SSH for Windows
- FTP/FTPD - MIT gssftp, ncftp, wu-ftpd ...
- Any other GSSAPI aware application
    - CORBA, SASL?

Delegation using Proxy Certificates

- Server creates key pair and certificate request, client signs request, returns certificate to server
- Subject name + CommonName “proxy”
- Passed by SSL in certificate chains
- GSI will accept a proxy as the user
  - Verifies the certificate chain
- Usable for process to process authentication
- Limited delegation - continuing research

Keys and Certificates



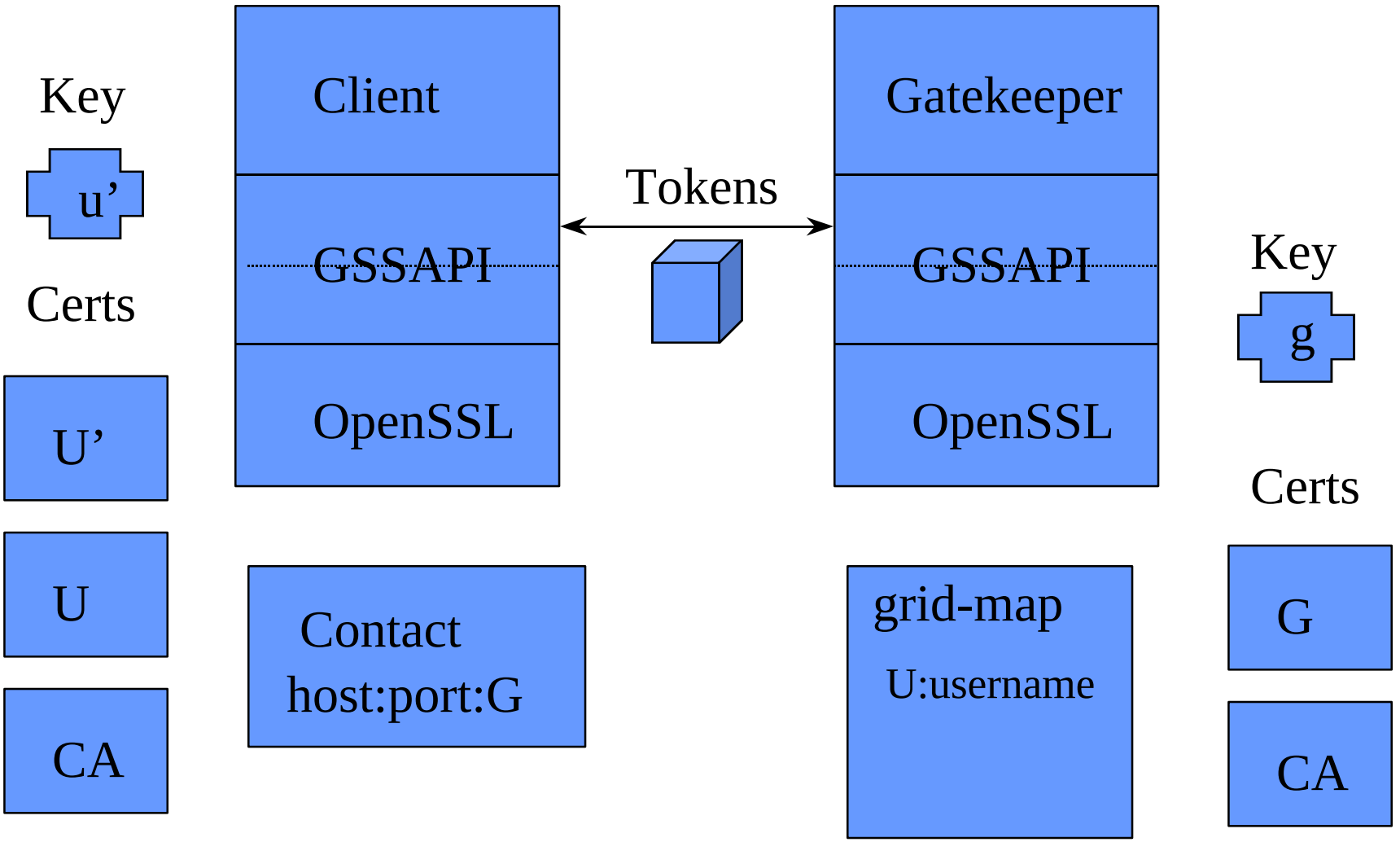
U'' - /C=US/O=Globus/.../CN=Doug/CN=proxy/CN=proxy

U' - /C=US/O=Globus/.../CN=Doug/CN=proxy

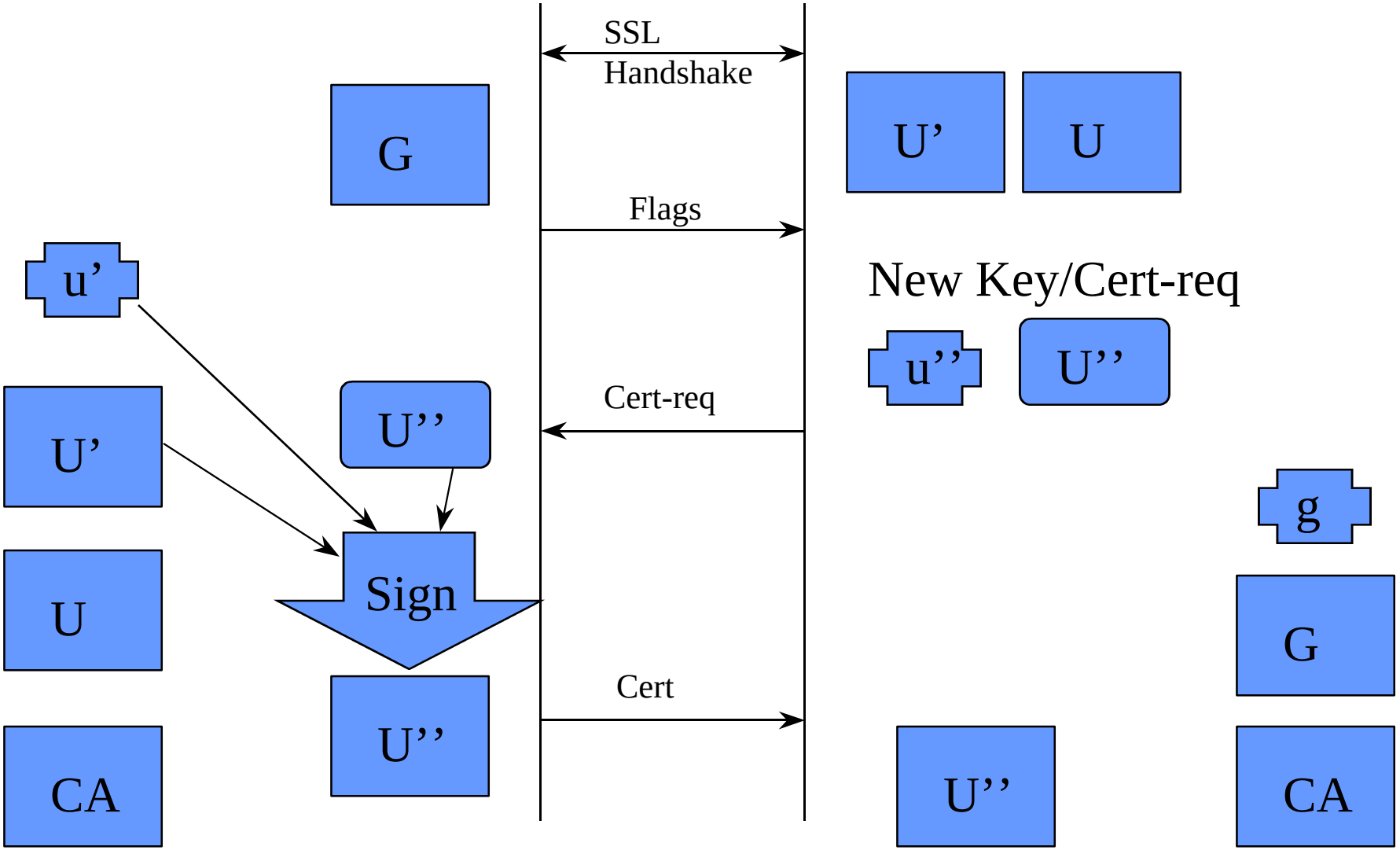
U - /C=US/O=Globus/.../CN=Doug

CA - /C=US/O=Globus/.../CN=Certificate Authority

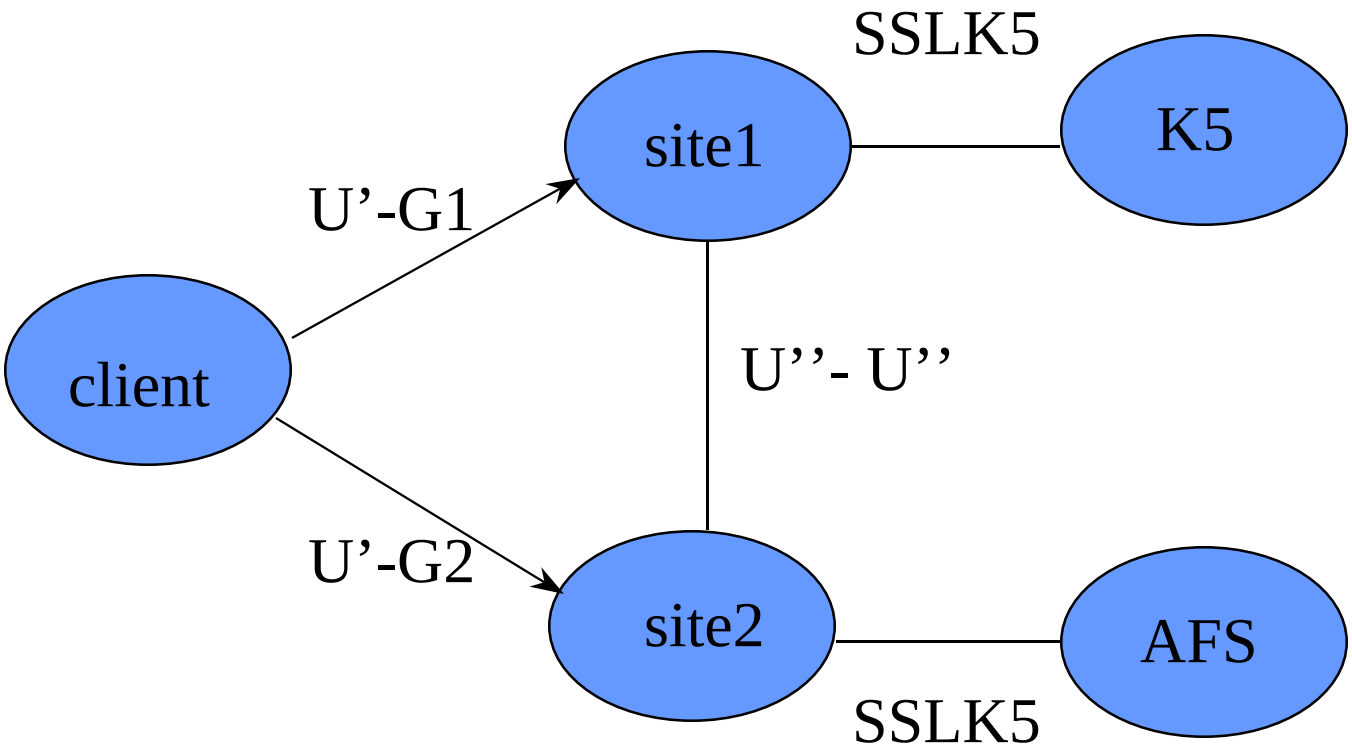
GSSAPI_SSLEAY - Proxy



GSSAPI_SSLEAY- Proxy



Local Site Authentication



Local Site Authorization

- Local accounts/username
  - Users arrange for this on their own
- Control access by local site
  - Gatekeeper/SSHD/FTPD/Server uses grid-map file to map certificate subject name to local userid

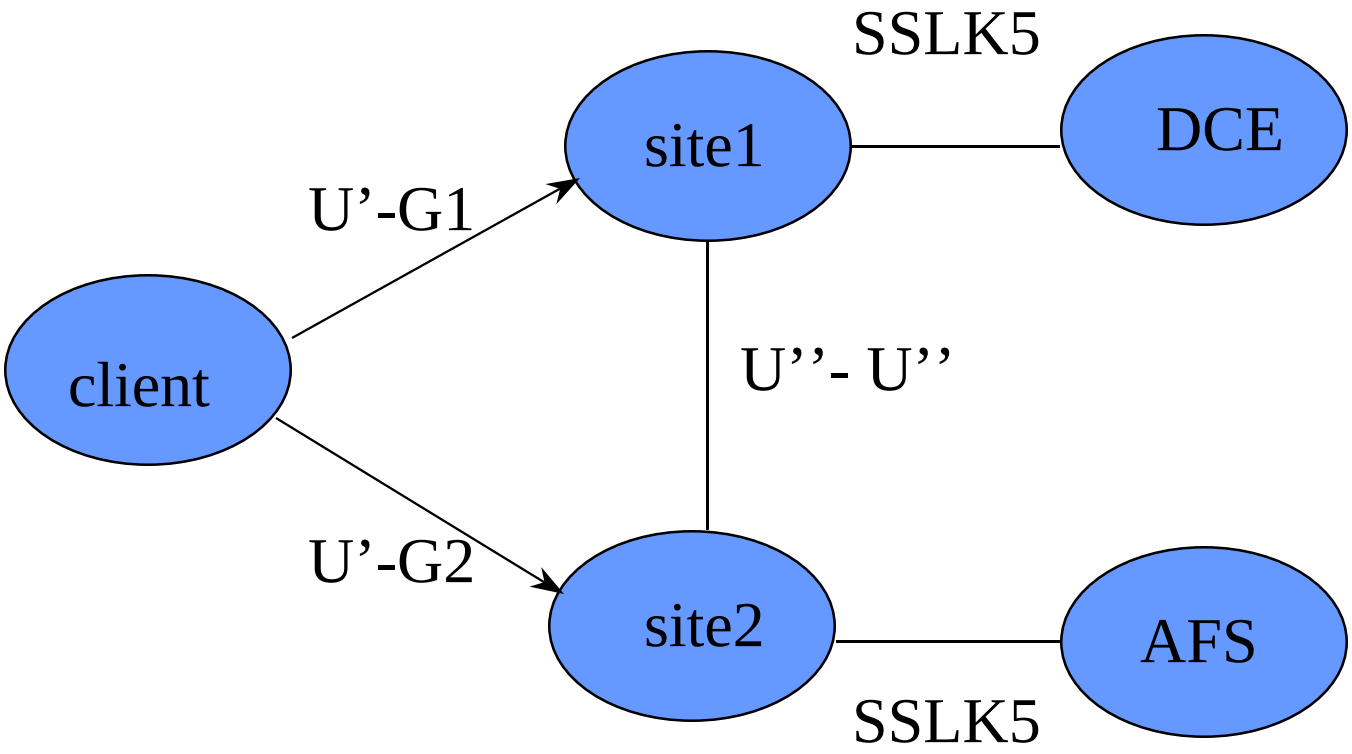
Interfacing to local site security infrastructures

- Kerberos, DCE and AFS
  - sslk5 - Use GSI certificates to get Kerberos ticket at local site Equivalent to PKINIT
  - K5cert uses Kerberos ticket to get short term certificate
- Entrust
  - Generate “Proxy” certificate (NASA - proof of concept)
- Secure-ID
  - SecureID gets Kerberos ticket
  - K5cert uses Kerberos ticket to get short term certificate
- Smart cards
  - PKCS#11 (Demonstrated at SC98) Uses same DLL as Netscape on Win32

K5cert to get a certificate

- K5cert authenticates to k5certd
  - User has Kerberos TGT:
  - b17783@dce.anl.gov
- K5certd acts as a CA
  - /C=US/O=Argonne National Laboratory/OU=Kerberos Realm dce.anl.gov/CN=Certificate Authority
- Issues certificate:
  - /C=US/O=Argonne National Laboratory/OU=Kerberos Realm dce.anl.gov/CN=b17783@dce.anl.gov
- Certificate lifetime = ticket lifetime

Local Site Authentication and user to user



the globus project
www.globus.org

GSI vs. Kerberos GSSAPI

- Certificate subject name
  - /O=Grid/O=Globus/CN=Doug Engert
  - /O=.../CN=host/cpu.anl.gov
- Grid-proxy-init
- Key and Certificate
- Delegation
- Proxy (key and certificate)
- CA (offline)
- Process-to-process - YES
- CRL

- Principal name
  - b17783@dce.anl.gov
  - host/cpu.anl.gov@dce.anl.gov
- kinit
- password or v5srvtab
- Forwarding
- Forwarded tickets
- KDC - online
- User-to-user - Almost
- Online KDC

the globus project
www.globus.org

Conclusions

- GSI is becoming widely accepted
- GSI uses well established security protocol
- GSI uses standard GSSAPI
- GSI can interface to current site security
- Delegation, across Kerberos and GSI
- Process -to-process authentication
- Local authorization and accounting
- Single sign-on

The End