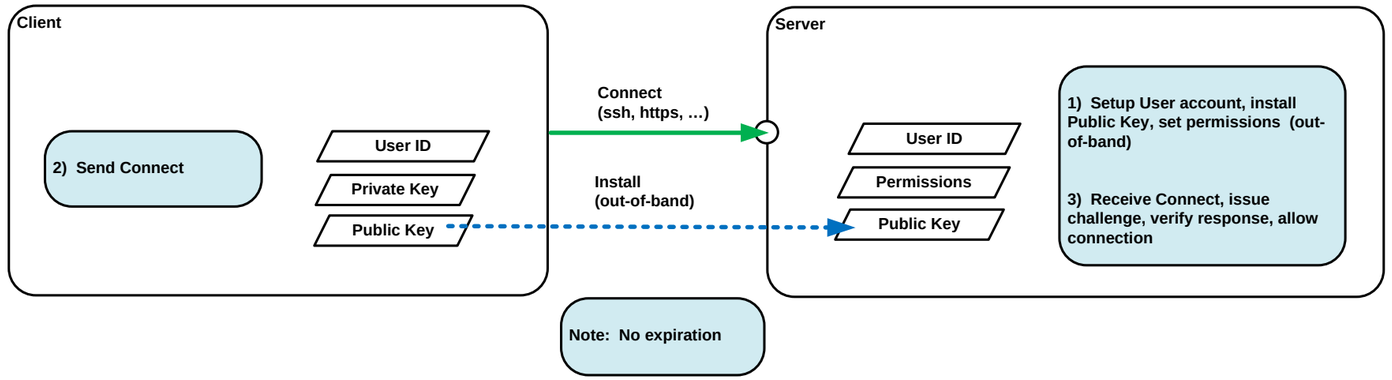
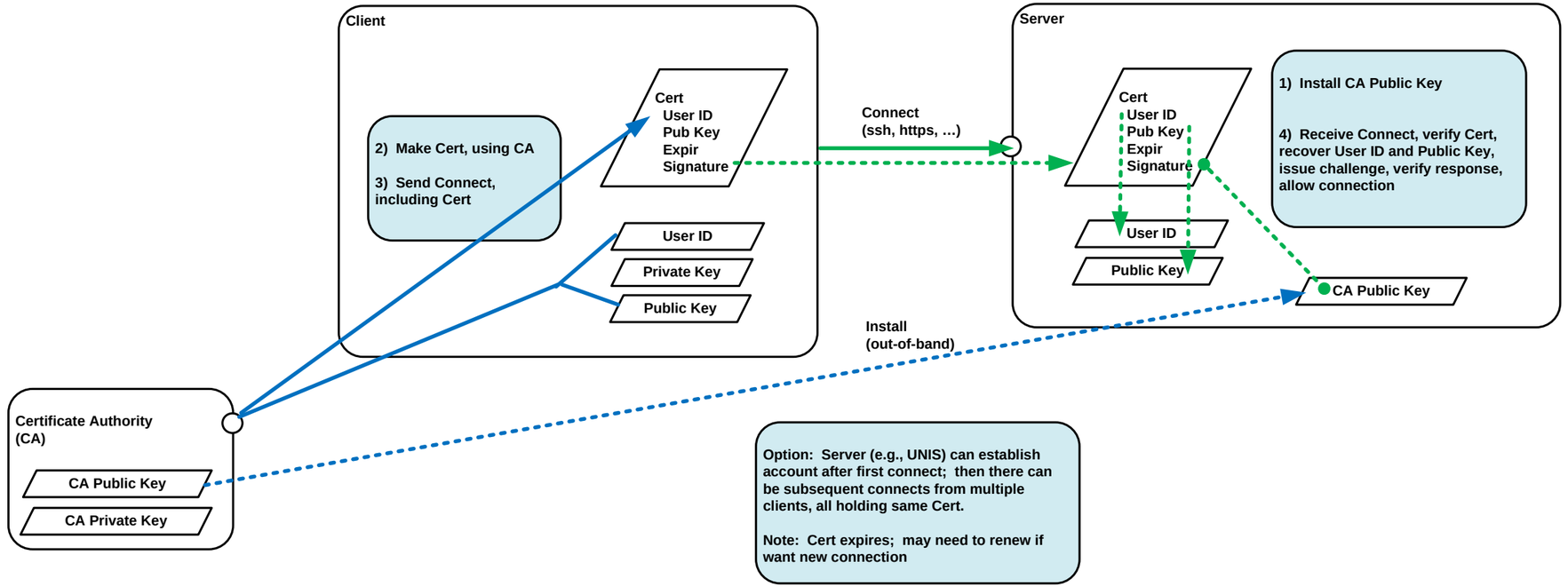
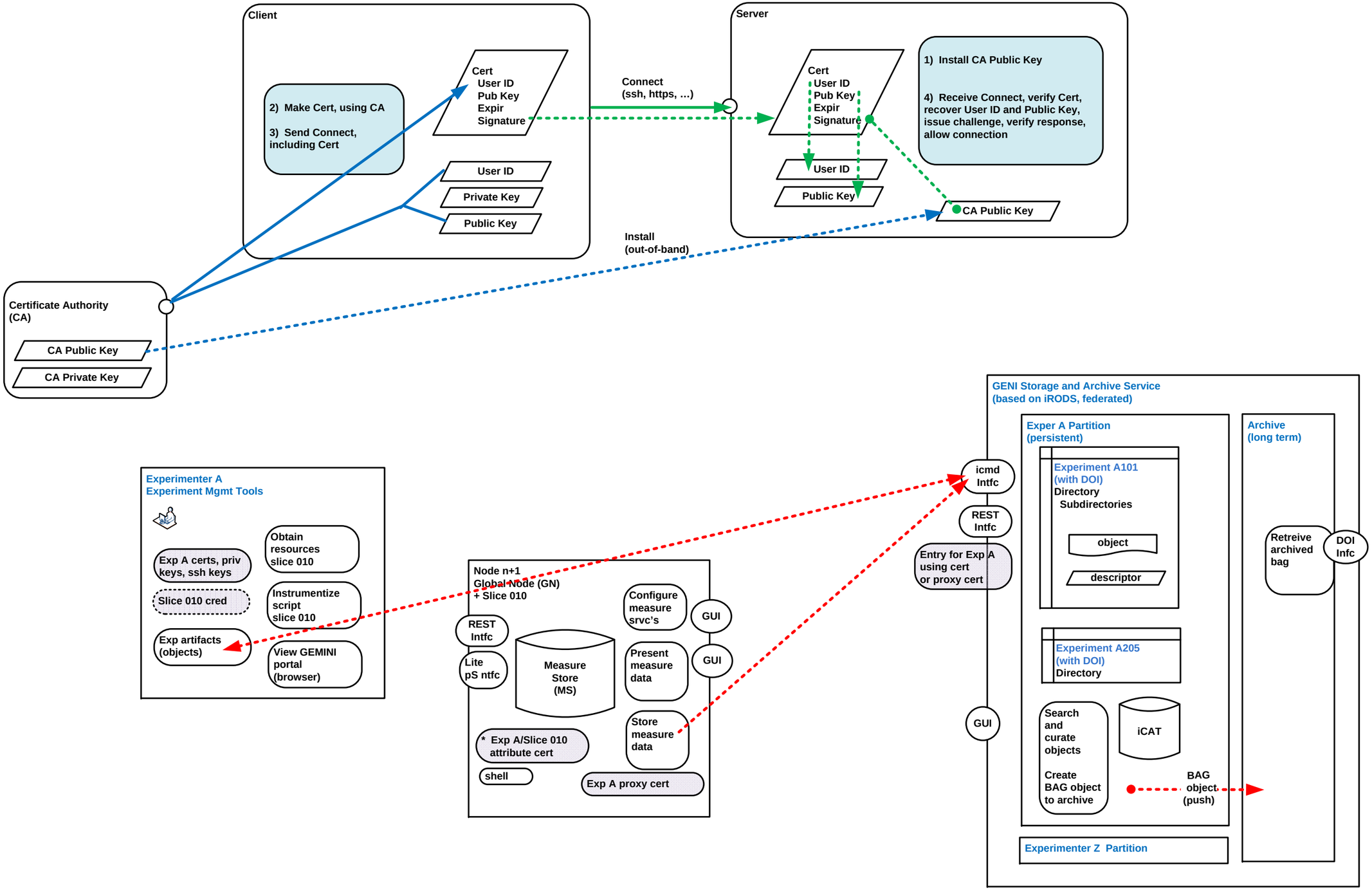
Case 1: Use Key Pair to Connect

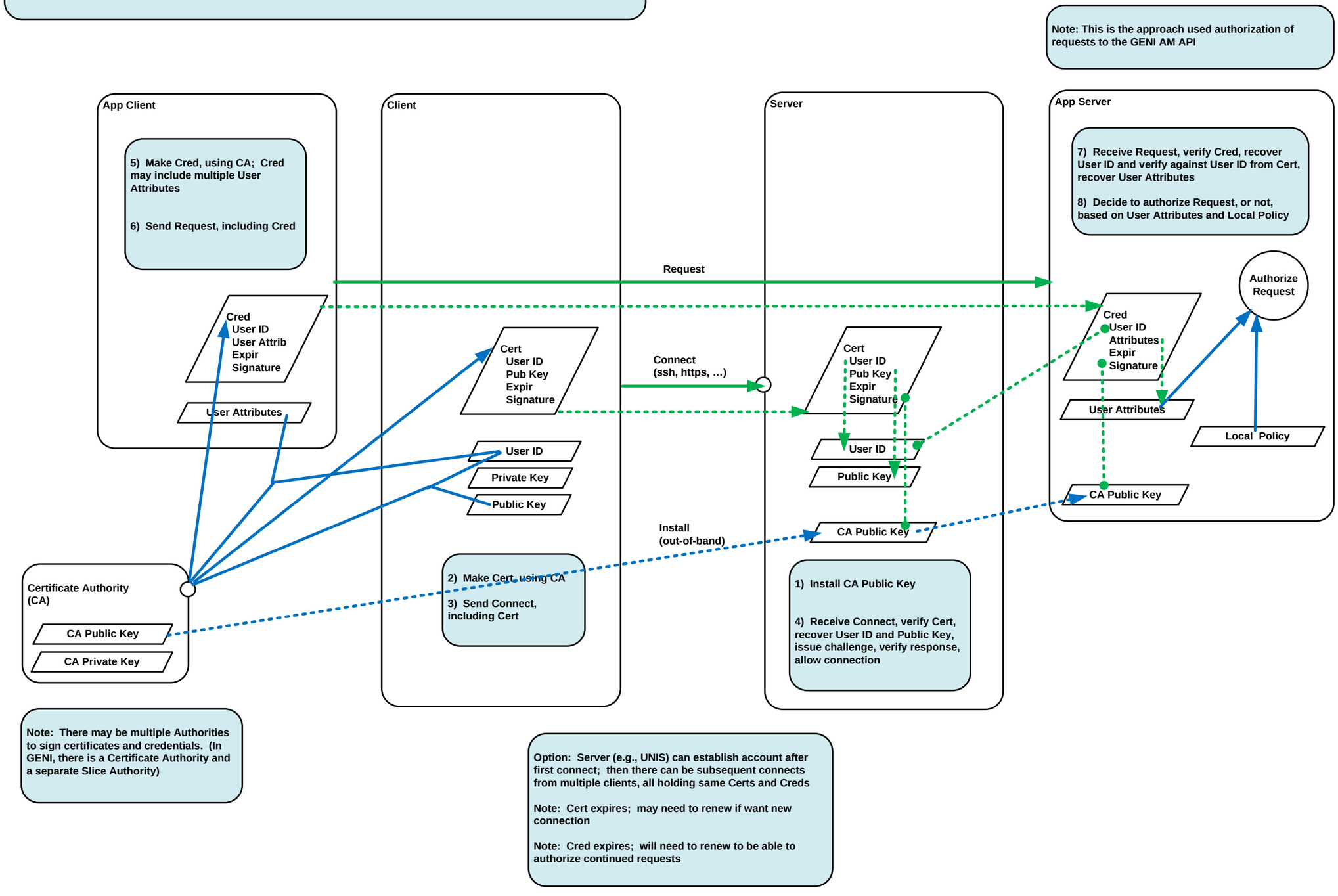


Case 1b: Use Certificate to Connect

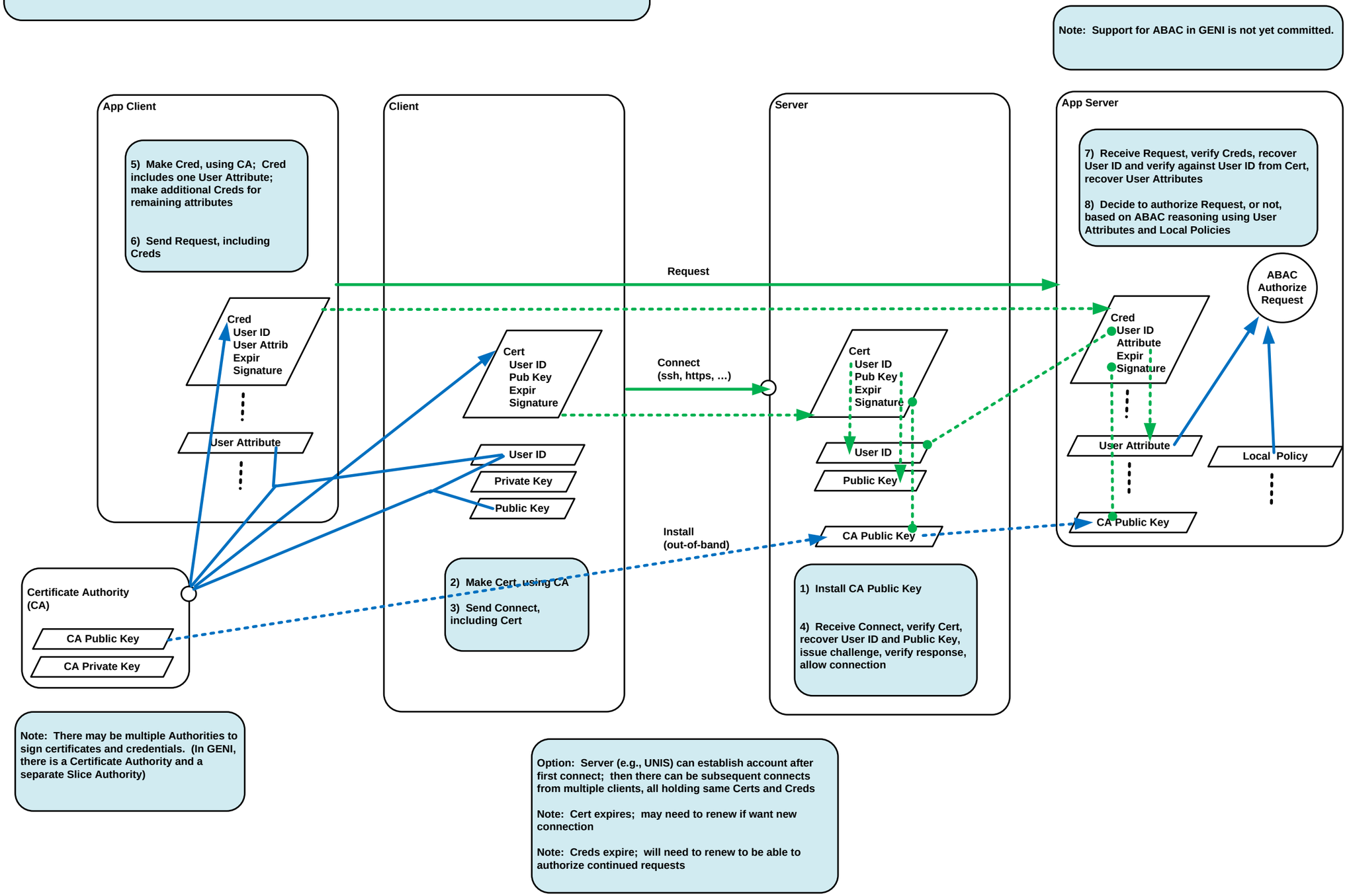


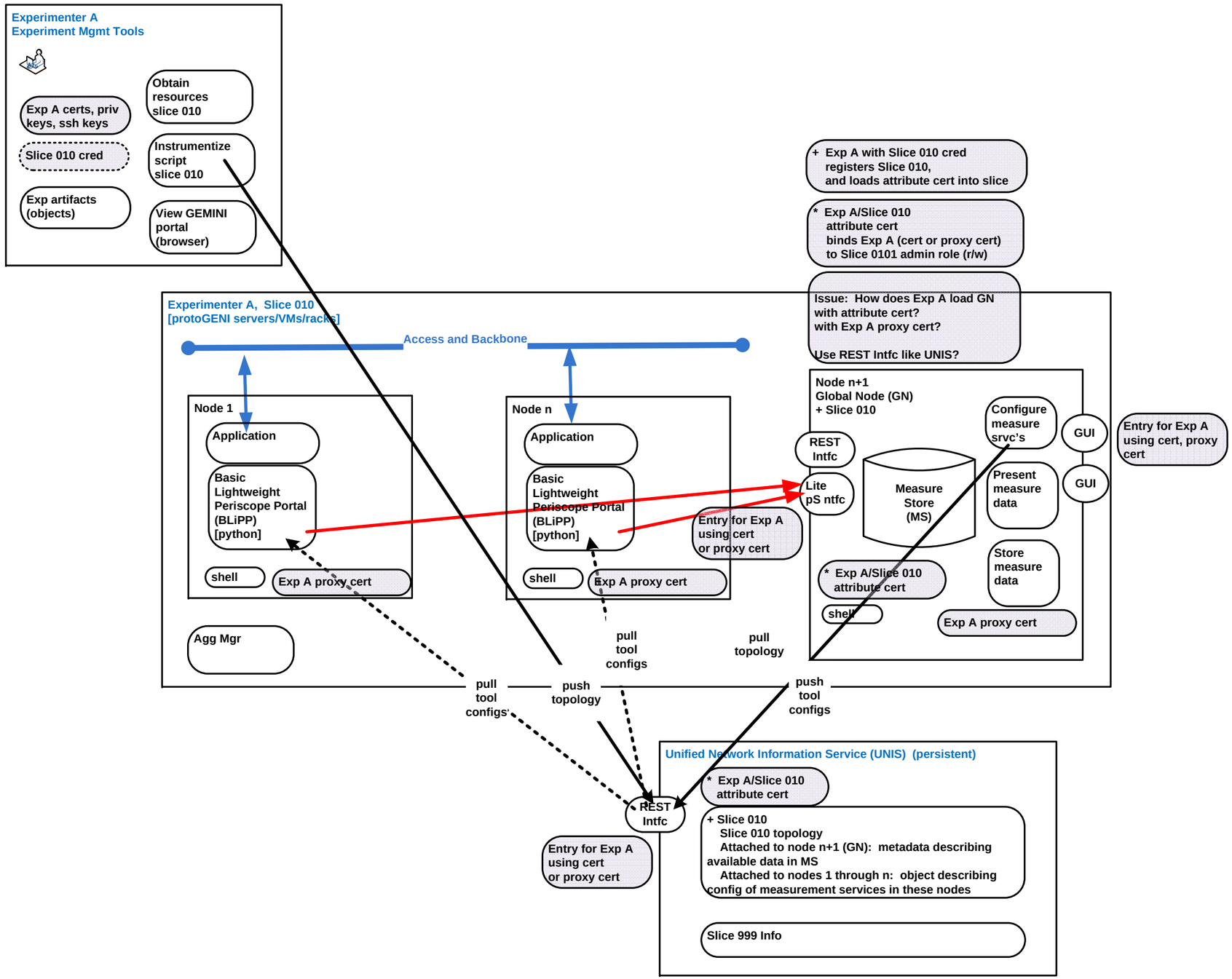

Client
2) Make Cert, using CA
3) Send Connect, including Cert
Cert
User ID
Pub Key
Expir
Signature
User ID
Private Key
Public Key
Connect
(ssh, https, ...)
Server
Cert
User ID
Pub Key
Expir
Signature
1) Install CA Public Key
4) Receive Connect, verify Cert, recover User ID and Public Key, issue challenge, verify response, allow connection
User ID
Public Key
CA Public Key
Install
(out-of-band)
Certificate Authority
(CA)
CA Public Key
CA Private Key
Experimenter A
Experiment Mgmt Tools
Exp A certs, priv keys, ssh keys
Slice 010 cred
Exp artifacts (objects)
Obtain resources slice 010
Instrumentize script slice 010
View GEMINI portal (browser)
Node n+1
Global Node (GN)
+ Slice 010
REST Intfc
Lite pS ntfc
Measure Store (MS)
Configure measure srvc's
GUI
Present measure data
GUI
Store measure data
* Exp A/Slice 010 attribute cert
shell
Exp A proxy cert
GENI Storage and Archive Service
(based on iRODS, federated)
icmd Intfc
REST Intfc
Entry for Exp A using cert or proxy cert
GUI
Exper A Partition
(persistent)
Experiment A101
(with DOI)
Directory
Subdirectories
object
descriptor
Experiment A205
(with DOI)
Directory
Search and curate objects
Create BAG object to archive
iCAT
BAG object (push)
Experimenter Z Partition
Archive
(long term)
Retreive archived bag
DOI Intfc

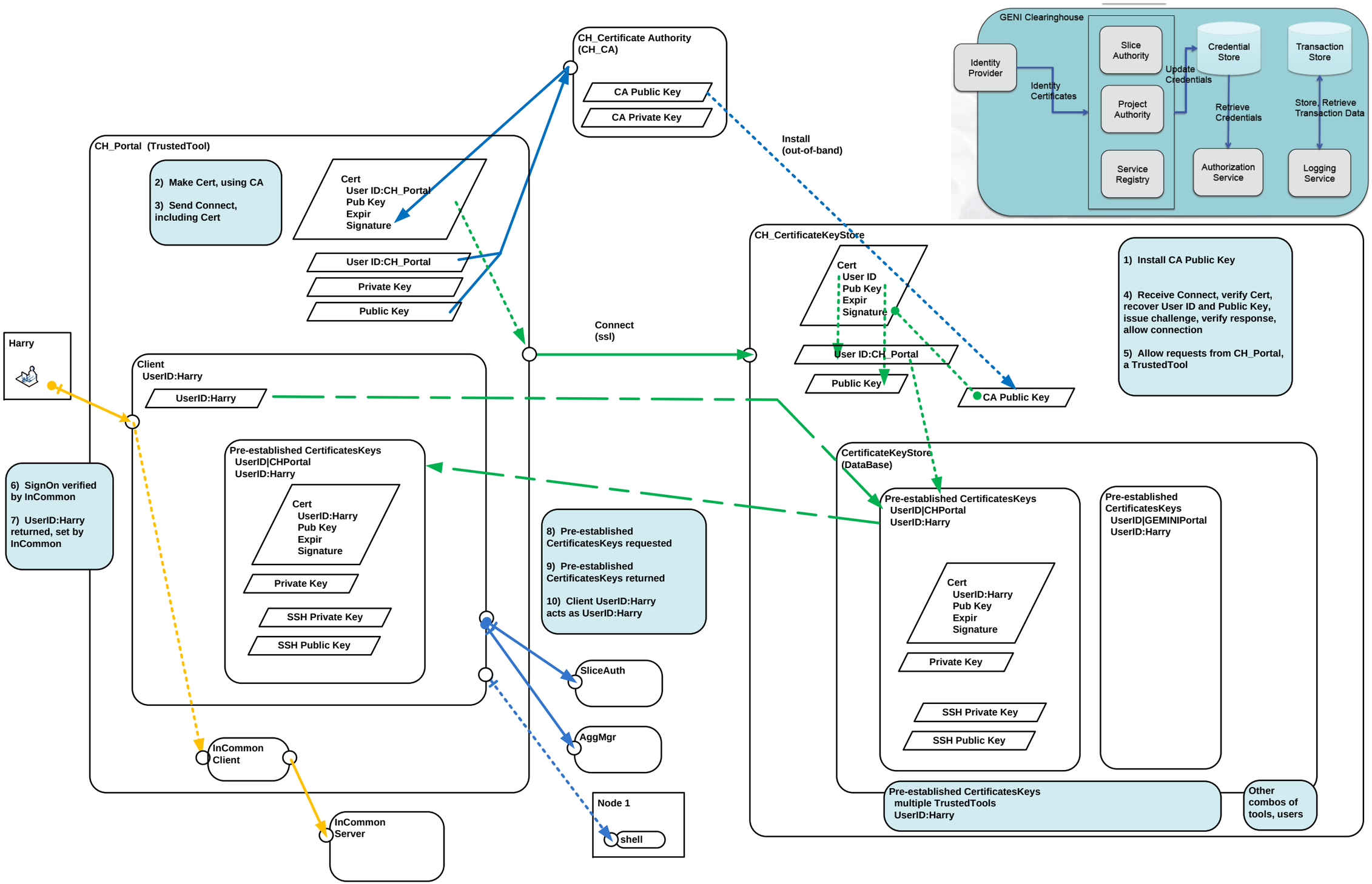
Case 2: Use Certificate to Connect, Credential to Authorize Request

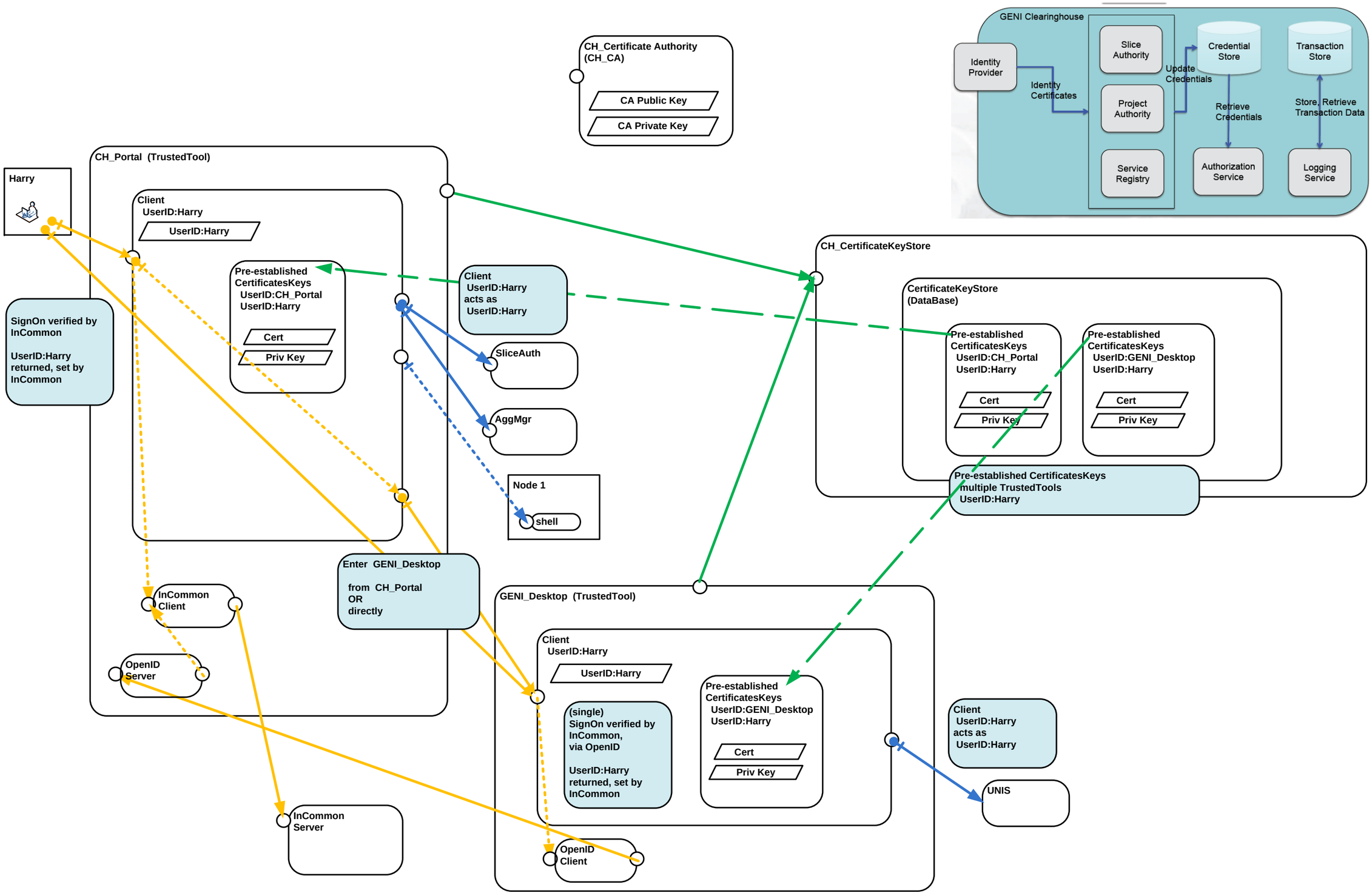


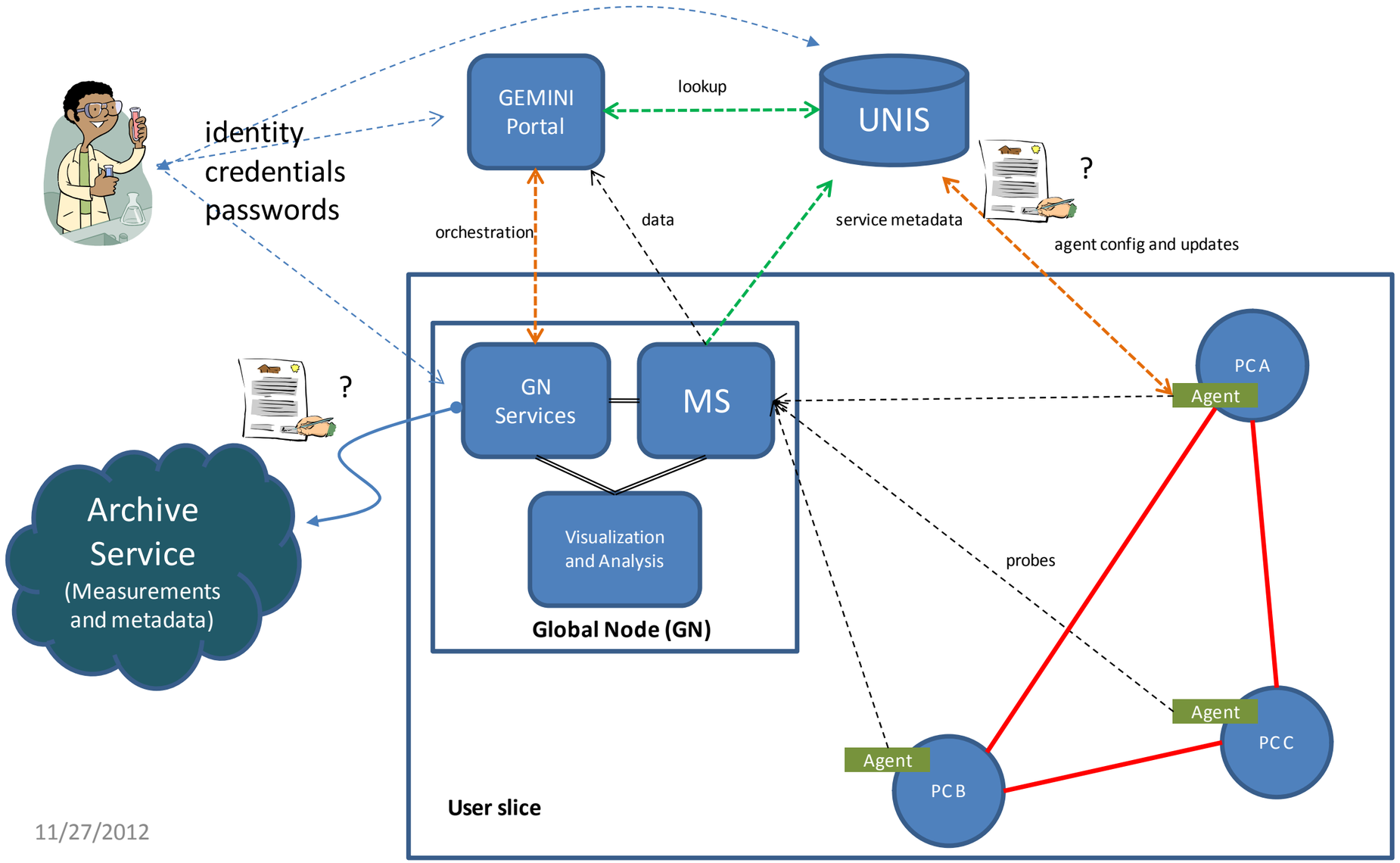
Case 2b: Use Certificate to Connect, ABAC to Authorize Request



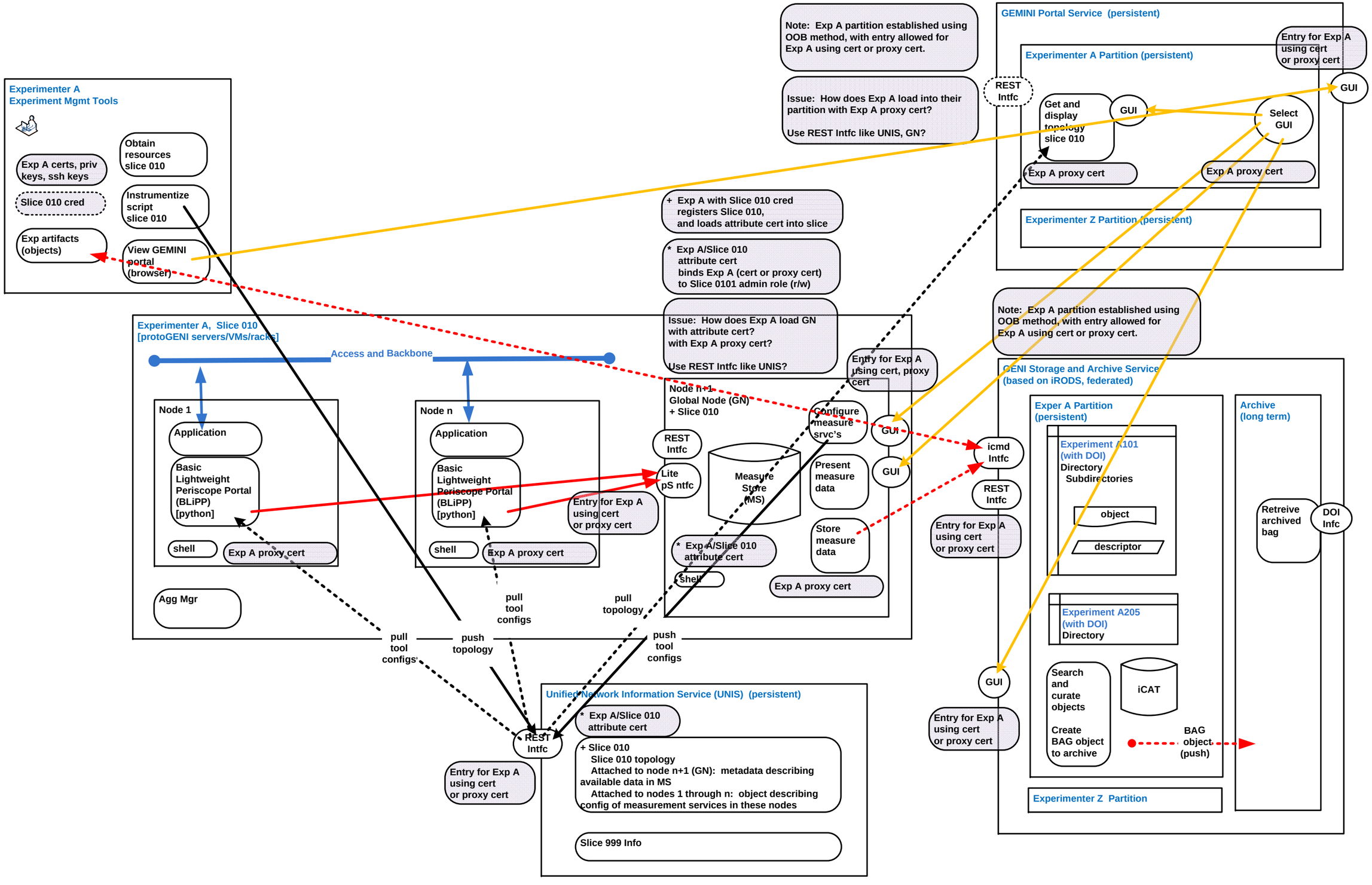

Experimenter A
Experiment Mgmt Tools
Exp A certs, priv keys, ssh keys
Slice 010 cred
Exp artifacts (objects)
Obtain resources slice 010
Instrumentize script slice 010
View GEMINI portal (browser)
+ Exp A with Slice 010 cred registers Slice 010, and loads attribute cert into slice
* Exp A/Slice 010 attribute cert binds Exp A (cert or proxy cert) to Slice 0101 admin role (r/w)
Issue: How does Exp A load GN with attribute cert? with Exp A proxy cert?
Use REST Intfc like UNIS?
Experimenter A, Slice 010
[protoGENI servers/VMs/racks]
Access and Backbone
Node 1
Application
Basic Lightweight Periscope Portal (BLiPP) [python]
shell
Exp A proxy cert
Node n
Application
Basic Lightweight Periscope Portal (BLiPP) [python]
shell
Exp A proxy cert
Entry for Exp A using cert or proxy cert
Node n+1
Global Node (GN)
+ Slice 010
REST Intfc
Lite pS ntfc
Measure Store (MS)
Configure measure srvc's
GUI
Entry for Exp A using cert, proxy cert
Present measure data
GUI
Store measure data
* Exp A/Slice 010 attribute cert
shell
Exp A proxy cert
Agg Mgr
pull tool configs
pull topology
pull tool configs
push topology
push tool configs
Unified Network Information Service (UNIS) (persistent)
* Exp A/Slice 010 attribute cert
REST Intfc
+ Slice 010
Slice 010 topology
Attached to node n+1 (GN): metadata describing available data in MS
Attached to nodes 1 through n: object describing config of measurement services in these nodes
Slice 999 Info
Entry for Exp A using cert or proxy cert

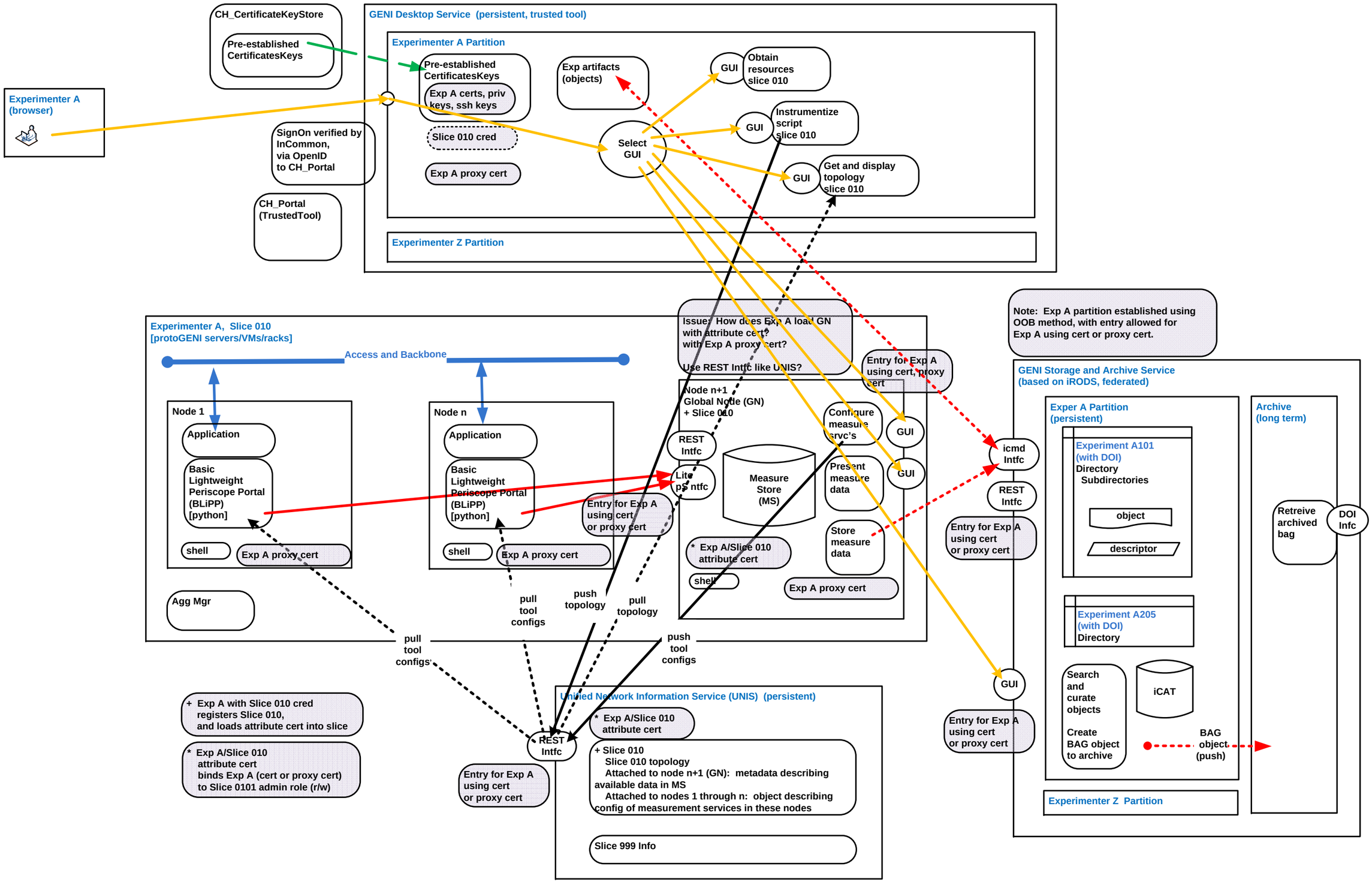

GENI Clearinghouse
Identity Provider
Identity Certificates
Slice Authority
Project Authority
Service Registry
Update Credentials
Credential Store
Retrieve Credentials
Authorization Service
Transaction Store
Store, Retrieve Transaction Data
Logging Service
CH_Certificate Authority (CH_CA)
CA Public Key
CA Private Key
Install (out-of-band)
CH_Portal (TrustedTool)
2) Make Cert, using CA
3) Send Connect, including Cert
Cert
User ID:CH_Portal
Pub Key
Expir
Signature
User ID:CH_Portal
Private Key
Public Key
Connect (ssl)
CH_CertificateKeyStore
Cert
User ID
Pub Key
Expir
Signature
User ID:CH_Portal
Public Key
CA Public Key
1) Install CA Public Key
4) Receive Connect, verify Cert, recover User ID and Public Key, issue challenge, verify response, allow connection
5) Allow requests from CH_Portal, a TrustedTool
Harry
Client
UserID:Harry
UserID:Harry
Pre-established CertificatesKeys
UserID|CHPortal
UserID:Harry
Cert
UserID:Harry
Pub Key
Expir
Signature
Private Key
SSH Private Key
SSH Public Key
6) SignOn verified by InCommon
7) UserID:Harry returned, set by InCommon
8) Pre-established CertificatesKeys requested
9) Pre-established CertificatesKeys returned
10) Client UserID:Harry acts as UserID:Harry
SliceAuth
AggMgr
InCommon Client
InCommon Server
Node 1
shell
CertificateKeyStore (DataBase)
Pre-established CertificatesKeys
UserID|CHPortal
UserID:Harry
Cert
UserID:Harry
Pub Key
Expir
Signature
Private Key
SSH Private Key
SSH Public Key
Pre-established CertificatesKeys
UserID|GEMINIPortal
UserID:Harry
Pre-established CertificatesKeys
multiple TrustedTools
UserID:Harry
Other combos of tools, users


GENI Clearinghouse
Identity Provider
Identity Certificates
Slice Authority
Project Authority
Service Registry
Update Credentials
Credential Store
Retrieve Credentials
Authorization Service
Transaction Store
Store, Retrieve Transaction Data
Logging Service
CH_Certificate Authority (CH_CA)
CA Public Key
CA Private Key
CH_Portal (TrustedTool)
Harry
Client
UserID:Harry
UserID:Harry
Pre-established CertificatesKeys
UserID:CH_Portal
UserID:Harry
Cert
Priv Key
SignOn verified by InCommon
UserID:Harry returned, set by InCommon
Client
UserID:Harry
acts as
UserID:Harry
SliceAuth
AggMgr
Node 1
shell
CH_CertificateKeyStore
CertificateKeyStore (DataBase)
Pre-established CertificatesKeys
UserID:CH_Portal
UserID:Harry
Cert
Priv Key
Pre-established CertificatesKeys
UserID:GENI_Desktop
UserID:Harry
Cert
Priv Key
Pre-established CertificatesKeys
multiple TrustedTools
UserID:Harry
Enter GENI_Desktop
from CH_Portal
OR
directly
InCommon Client
OpenID Server
InCommon Server
GENI_Desktop (TrustedTool)
Client
UserID:Harry
UserID:Harry
(single) SignOn verified by InCommon, via OpenID
UserID:Harry returned, set by InCommon
Pre-established CertificatesKeys
UserID:GENI_Desktop
UserID:Harry
Cert
Priv Key
OpenID Client
Client
UserID:Harry
acts as
UserID:Harry
UNIS


identity
credentials
passwords
GEMINI Portal
lookup
UNIS
?
orchestration
data
service metadata
agent config and updates
?
GN Services
MS
Visualization and Analysis
Global Node (GN)
PCA
Agent
probes
Agent
PCC
Agent
PCB
User slice
Archive Service
(Measurements and metadata)

11/27/2012


Experimenter A
Experiment Mgmt Tools
Exp A certs, priv keys, ssh keys
Slice 010 cred
Exp artifacts (objects)
Obtain resources slice 010
Instrumentize script slice 010
View GEMINI portal (browser)
Note: Exp A partition established using OOB method, with entry allowed for Exp A using cert or proxy cert.
Issue: How does Exp A load into their partition with Exp A proxy cert?
Use REST Intfc like UNIS, GN?
REST Intfc
GEMINI Portal Service (persistent)
Entry for Exp A using cert or proxy cert
Experimenter A Partition (persistent)
GUI
Get and display topology slice 010
GUI
Select GUI
Exp A proxy cert
Exp A proxy cert
Experimenter Z Partition (persistent)
+ Exp A with Slice 010 cred registers Slice 010, and loads attribute cert into slice
* Exp A/Slice 010 attribute cert binds Exp A (cert or proxy cert) to Slice 0101 admin role (r/w)
Issue: How does Exp A load GN with attribute cert? with Exp A proxy cert?
Use REST Intfc like UNIS?
Note: Exp A partition established using OOB method, with entry allowed for Exp A using cert or proxy cert.
Experimenter A, Slice 010
[protoGENI servers/VMs/racks]
Access and Backbone
Node 1
Application
Basic Lightweight Periscope Portal (BLiPP) [python]
shell
Exp A proxy cert
Node n
Application
Basic Lightweight Periscope Portal (BLiPP) [python]
shell
Exp A proxy cert
Entry for Exp A using cert or proxy cert
Agg Mgr
Node n+1 Global Node (GN) + Slice 010
REST Intfc
Lite pS ntfc
Measure Store (MS)
Configure measure srvc's
GUI
GUI
Present measure data
Store measure data
* Exp A/Slice 010 attribute cert
shell
Exp A proxy cert
Entry for Exp A using cert, proxy cert
GENI Storage and Archive Service (based on iRODS, federated)
Exper A Partition (persistent)
Experiment A101 (with DOI)
Directory
Subdirectories
object
descriptor
Experiment A205 (with DOI)
Directory
Search and curate objects
Create BAG object to archive
iCAT
BAG object (push)
Archive (long term)
Retreive archived bag
DOI Intfc
Experimenter Z Partition
icmd Intfc
REST Intfc
Entry for Exp A using cert or proxy cert
GUI
Entry for Exp A using cert or proxy cert
pull tool configs
push topology
pull topology
push tool configs
pull tool configs
Unified Network Information Service (UNIS) (persistent)
* Exp A/Slice 010 attribute cert
REST Intfc
+ Slice 010
Slice 010 topology
Attached to node n+1 (GN): metadata describing available data in MS
Attached to nodes 1 through n: object describing config of measurement services in these nodes
Slice 999 Info
Entry for Exp A using cert or proxy cert


CH_CertificateKeyStore
Pre-established CertificatesKeys
GENI Desktop Service (persistent, trusted tool)
Experimenter A Partition
Pre-established CertificatesKeys
Exp A certs, priv keys, ssh keys
Slice 010 cred
Exp A proxy cert
Exp artifacts (objects)
GUI
Obtain resources slice 010
GUI
Instrumentize script slice 010
GUI
Get and display topology slice 010
Select GUI
Experimenter A (browser)
SignOn verified by InCommon, via OpenID to CH_Portal
CH_Portal (TrustedTool)
Experimenter Z Partition
Experimenter A, Slice 010 [protoGENI servers/VMs/racks]
Access and Backbone
Node 1
Application
Basic Lightweight Periscope Portal (BLiPP) [python]
shell
Exp A proxy cert
Node n
Application
Basic Lightweight Periscope Portal (BLiPP) [python]
shell
Exp A proxy cert
Agg Mgr
Entry for Exp A using cert or proxy cert
Issues: How does Exp A load GN with attribute cert? with Exp A proxy cert?
Use REST Intfc like UNIS?
Node n+1 Global Node (GN) + Slice 010
REST Intfc
Lite ps ntfc
Measure Store (MS)
Configure measure srvc's
GUI
Present measure data
GUI
Store measure data
* Exp A/Slice 010 attribute cert
shell
Exp A proxy cert
Entry for Exp A using cert or proxy cert
pull tool configs
push topology
pull topology
pull tool configs
push tool configs
Note: Exp A partition established using OOB method, with entry allowed for Exp A using cert or proxy cert.
GENI Storage and Archive Service (based on iRODS, federated)
Exper A Partition (persistent)
Experiment A101 (with DOI)
Directory
Subdirectories
object
descriptor
Experiment A205 (with DOI)
Directory
Search and curate objects
Create BAG object to archive
iCAT
BAG object (push)
Archive (long term)
Retreive archived bag
DOI Intfc
Experimenter Z Partition
icmd Intfc
REST Intfc
Entry for Exp A using cert or proxy cert
GUI
Entry for Exp A using cert or proxy cert
+ Exp A with Slice 010 cred registers Slice 010, and loads attribute cert into slice
* Exp A/Slice 010 attribute cert binds Exp A (cert or proxy cert) to Slice 0101 admin role (r/w)
Unified Network Information Service (UNIS) (persistent)
* Exp A/Slice 010 attribute cert
REST Intfc
Entry for Exp A using cert or proxy cert
+ Slice 010
Slice 010 topology
Attached to node n+1 (GN): metadata describing available data in MS
Attached to nodes 1 through n: object describing config of measurement services in these nodes
Slice 999 Info