LHCONE Point-to-Point Circuit Experiment

Authentication and Authorization Model Discussion

LHCONE meeting, Rome April 28-29, 2014

W. Johnston, Senior Scientist and Advisor

ESnet and Lawrence Berkeley National Laboratory

Berkeley, California, U.S.A

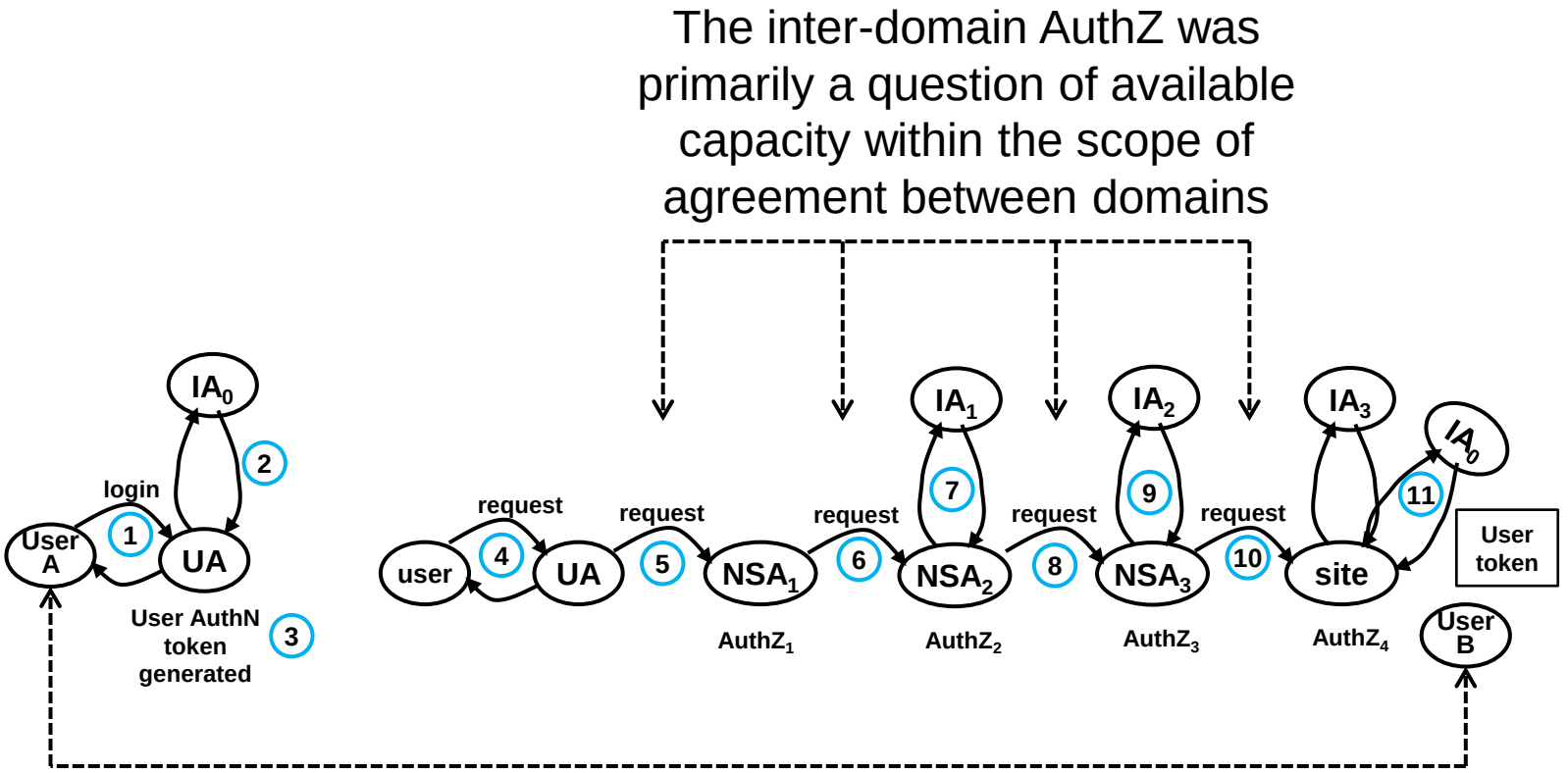
AuthN/AuthZ simplicity is essential

- Very important to keep the authentication (AuthN) and authorization (AuthZ) as simple as possible during the experiment phase: NSI deployment and interopability testing
  - We need to focus initially on making sure that the Provider NSAs will work together and reliability setup nad operate multi-domain circuits
- On the other hand, it should not be ignored because somthting will have to be in place when end sites start using the service, even experimentally
- One way to keep AuthN as simple as possible is to have all those operations done in as small a trust sphere as possible
- A simple authorization environment will also help to keep authenticaion simple
  - For example:
  - Only have the requesting user authorized by the first domain encountered (e.g. the upstream NSP)
  - During circuit setup, the NSPs only authorize to each other (chain model)

AuthN/AuthZ simplicity is essential

- The IDCP only supported a chain model of multi-domain VC set up
  - AuthZ was essentially first-come, first-served basis
  - The NSPs had agreements among themselves about how much guaranteed b/w traffic that they are willing to carry and the end user identities were not relevant beyond the first domain
  - The users at each end could verify the identity of the other – the ultimate AuthZ was whether the user at the far end from the requestor was willing to allow the circuit to be built at the receiving site
- However, the chain model of set up across multiple domains is fragile and prone to stalling for reasons that cannot be determined by the requestor

Chain model of circuit setup and AuthN/AuthZ

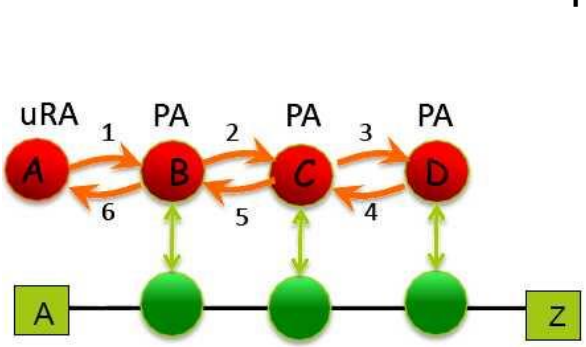


The "ultimate" AuthZ is essentially an out-of-band, bi-lateral agreement between UserA and UserB

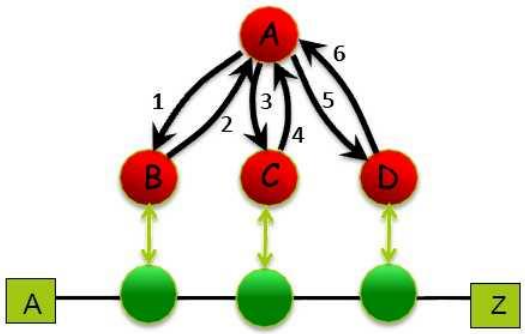
- This is effectively how Authn/AuthZ was implemented in IDCP and is probably the simplist model as identity verification is kept mostly local

LHCONE P2P Issues and Required Functionality

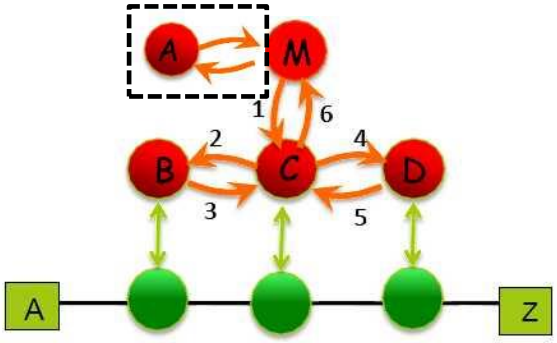
Several models have been proposed for constructing the inter-domain connection /3/



Chain model



Tree model



3rd party request

What are the issues with these models and what lessons can we draw for the LHCONE P2P service?

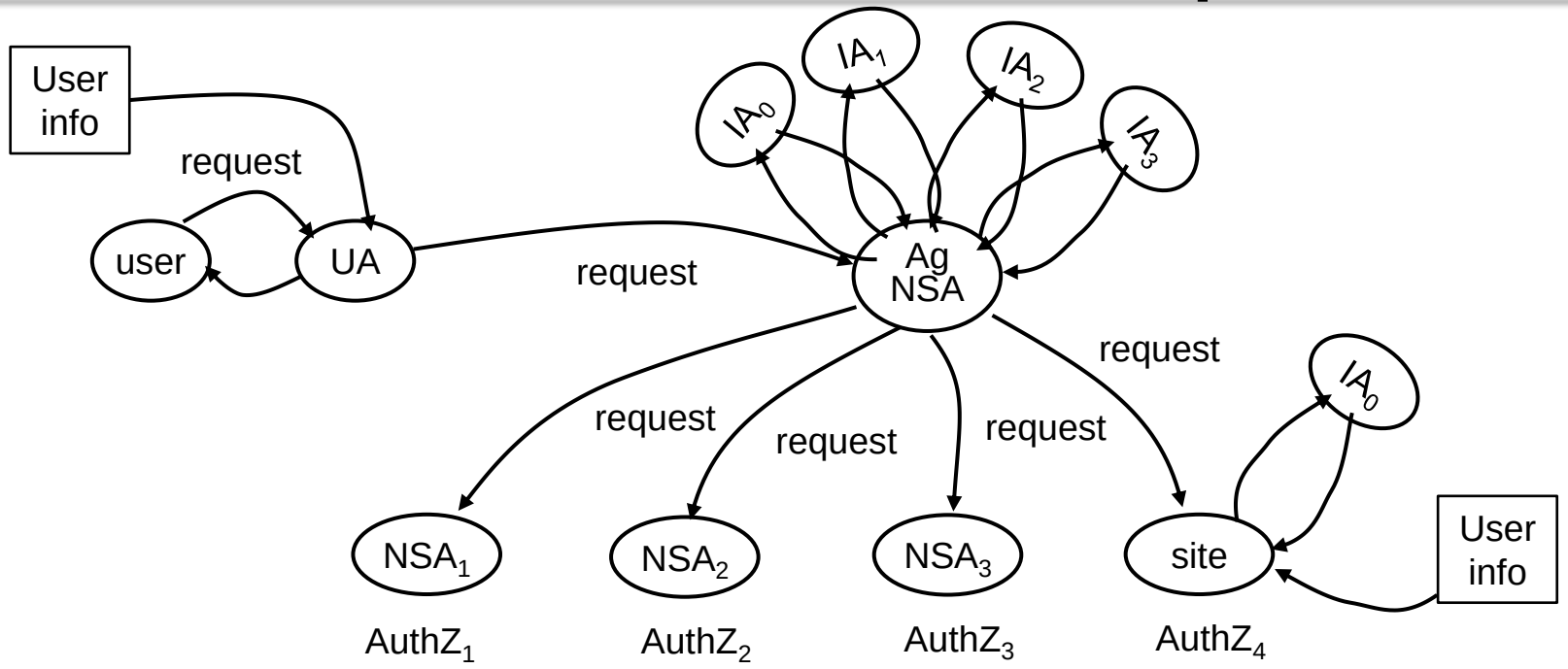
- The *chain model* is inherently slow and un-scalable with the current generation of software
- The *tree model* requires the user to have standing with all the intermediate domains, which will almost certainly never be the case
- The *3rd party request model* seems most likely to be successful – probably in a tree model configuration because
  - The connection setup requests to the intermediate domains can be handled in parallel
  - The user only has to have standing with a single entity (“M”) that could be a community service (M then has standing with all possible intermediate networks
  - “M” then is likely the NSA acting as an aggregation service
- All of these assume discovery and topology services are in place

/3/ “GLIF Automated GOLE Pilot Project and NSI,” Sobieski. LHCONE Meeting, Jan 30/31, 2012, Berkeley, USA

AuthN/AuthZ simplicity is essential

- The ability of the NSI Aggregrator to function in tree mode is designed to address the fragility of the chain model
  - The Aggregrator can see what is happening in the requested setup of each segment of the multi-domain path and when problems develop on one segment, can use its global path-finding ability to see if other routes are available
  - The concept of an “aggregrator” is the single functional improvement of NSI over IDCP
  - Use of the Aggregrator in tree mode is likely critical for the success of the LHCONE P2P environment, so a minimalist AuthN/AuthZ model that accommodates the Aggregrator must be developed
    - E.g. have an LHC specialized Aggregrator act as the 3rd party noted above so that the user does not have to authenticate or authorize with intermediate domains

Tree model of circuit setup



- This model concentrates all trust management with the Aggregrator and has several characteristics
  - The AG must be able to verify the idenitiy of everyone
  - The AG can effectively define a distinct user community (e.g. LHC) if the NSPs support multiple science communities
    - That is, the AG can be “owned” by the LHC community
- This is a more complicated trust model than chain, but the tree management of VC setup is essential

Resource Management and AuthZ

- No model exists for fine-grained management of b/w resources
  - I commented on an Arch call that I would see how ESnet scheduled its 100G and OpenFlow testbeds
  - Brian Tierney said that they considered partial resource allocation, but decided it was not worth the effort: The testebds are scheduled as a whole unit