Token Based GMPLS

Research into optical network architectures using Token Based access control, path authorization and resource management methods.

7th Annual Global LambdaGrid Workshop - Prague 17-09-2007

Leon Gommans - University of Amsterdam

Acknowledgements: Marten Hoekstra, Fred Wan, Li Xu, Yuri Demchenko, Mihai Cristea, Paola Grosso, Jeroen van de Ham, Freek Dijkstra, Arie Taal, Bert Andree, Cees de Laat, Bob Hulsenbosch, Robert de Groote, John Vollbrecht, Tom Lehman, Jerry Sobieski, Chris Tracy, Andrew Lake, Inder Monga

UNIVERSITEIT VAN AMSTERDAM

Content

Token Rationale / Single domain – Multi domain.

Context – demo setup for SC 07

Grid style and Provider style UNI

Consequences for the domain controller UNI

Token mechanism implementations

How to communicate tokens or token keys amongst domains

Implementation within OSCARS / & DRAGON GMPLS

Tokens are a **simple** way to provide service access, decoupling Purchase (Authorization) and Usage
Network projects look at how to integrate Authorization

Pitlochry, Scotland - Summer 2005
Sign in front of a liquor store

In railways, tokens or tickets allow recognition of legitimate passengers when public access is possible

The analogy with Optical Networking:

1. A Network Resource Provisioning System (NRPS) or Inter Domain Controllers (IDC), InterDomain Managers (IDMs) etc. “schedule the trains” (the lightpath reservations)

An IDC/IDM/NRPSs etc. however, **does not enforce access** for a particular “passenger” (ie user session) - “the train runs with or without passengers”.

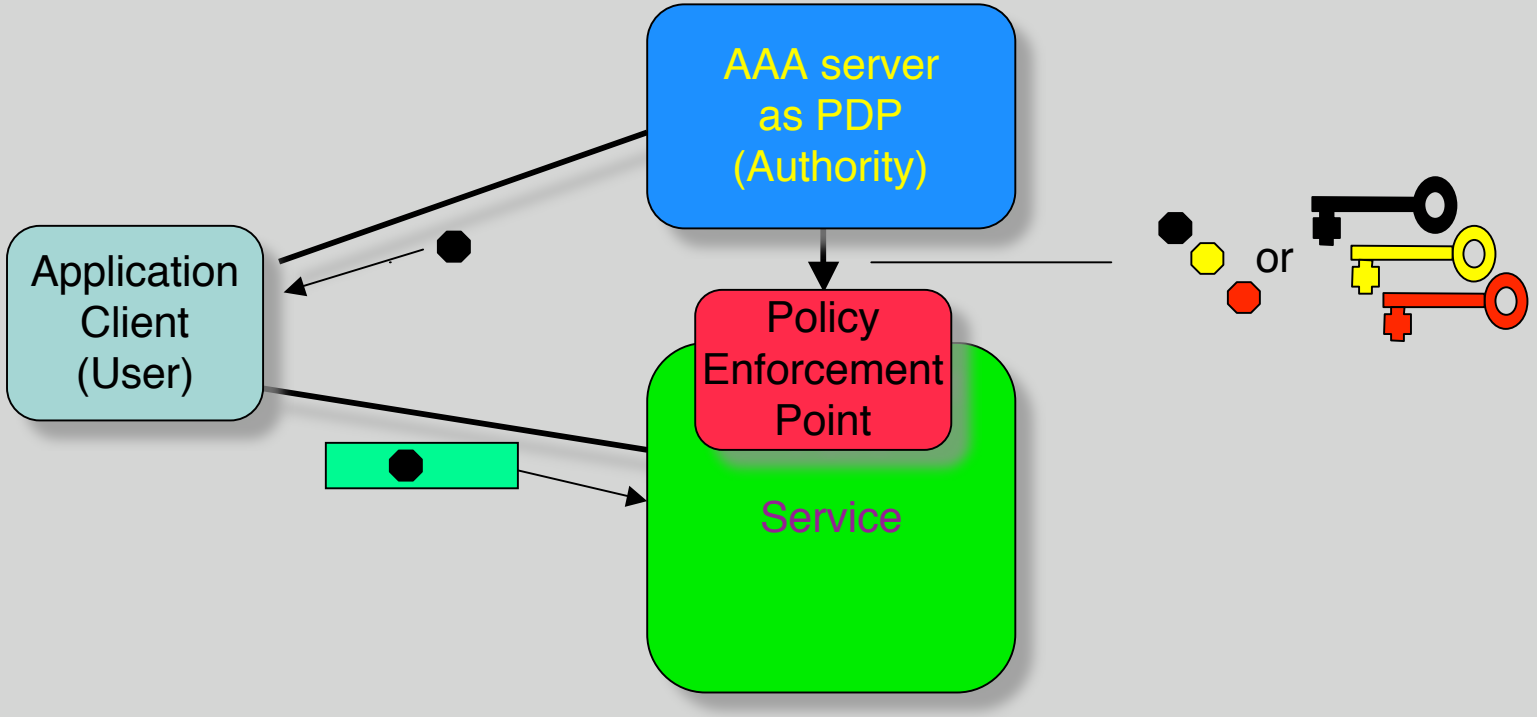
Access control is important if a network resources are offered as public service.

A token or ticket symbolizes the **history** that a passenger has obtained the right to access the service by having paid the appropriate fare. Also allows **simple validity check anywhere** during travel.

Token / ticket enables easy recognition of passengers in multi-domain scenarios

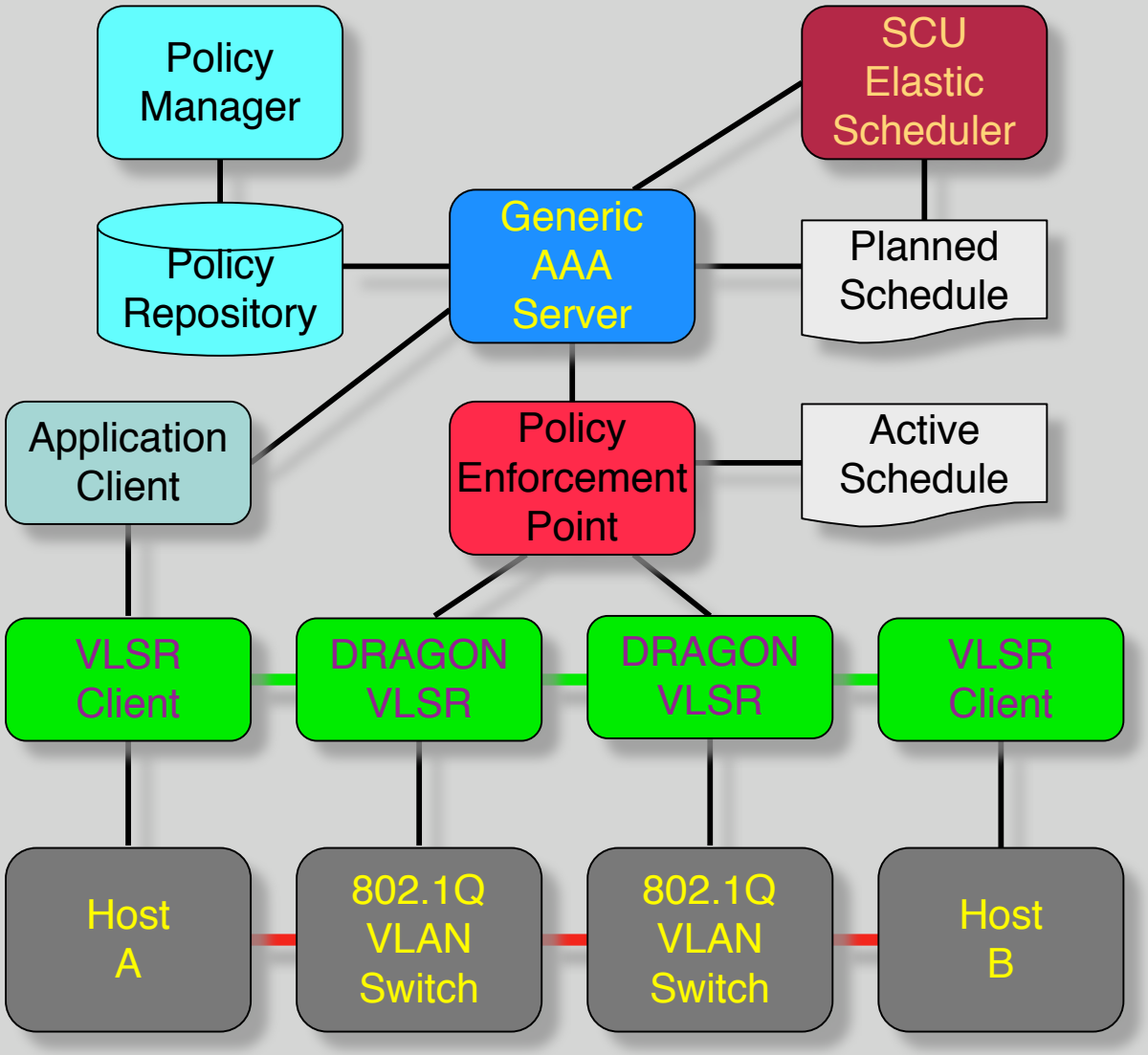
- Once the path is clear, a (set of-) querie(s) to a individual Domain Controller (DC) fits the request to network resource in time domain.
- Each DC must (together) create a service reference, identifying the agreed service which could be carried as part of the ticket / token information during travel.
- DC must have interface such that agents or peer DCs can obtain **references** for each individual domain (Local Resource Identifier - LRI) or use an agreed global reference (Global Resource Indentifier - GRI)
- Each domain must at least be able to recognize the **authenticity of this reference** to make sure the passenger is legitimate. An Authority, which signs the reference, will bind the lightpath request to the committed resources for a particular (planned) user session.

The Token Model - a step back to the RFC 2904 Push Model



Token associated with a Service Identifier

Single domain demo at SC 06

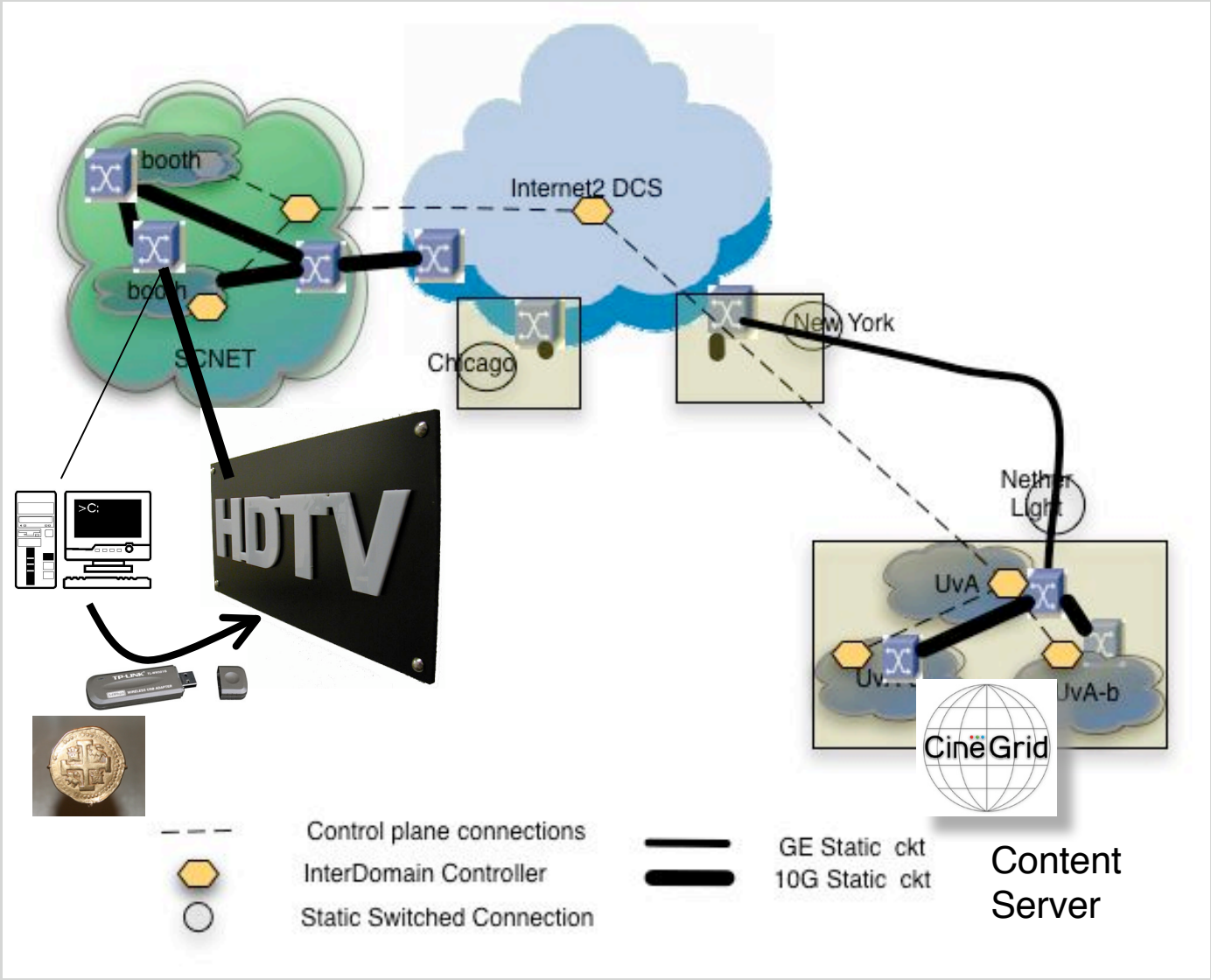


Results of SC 06 demo and meetings thereafter.

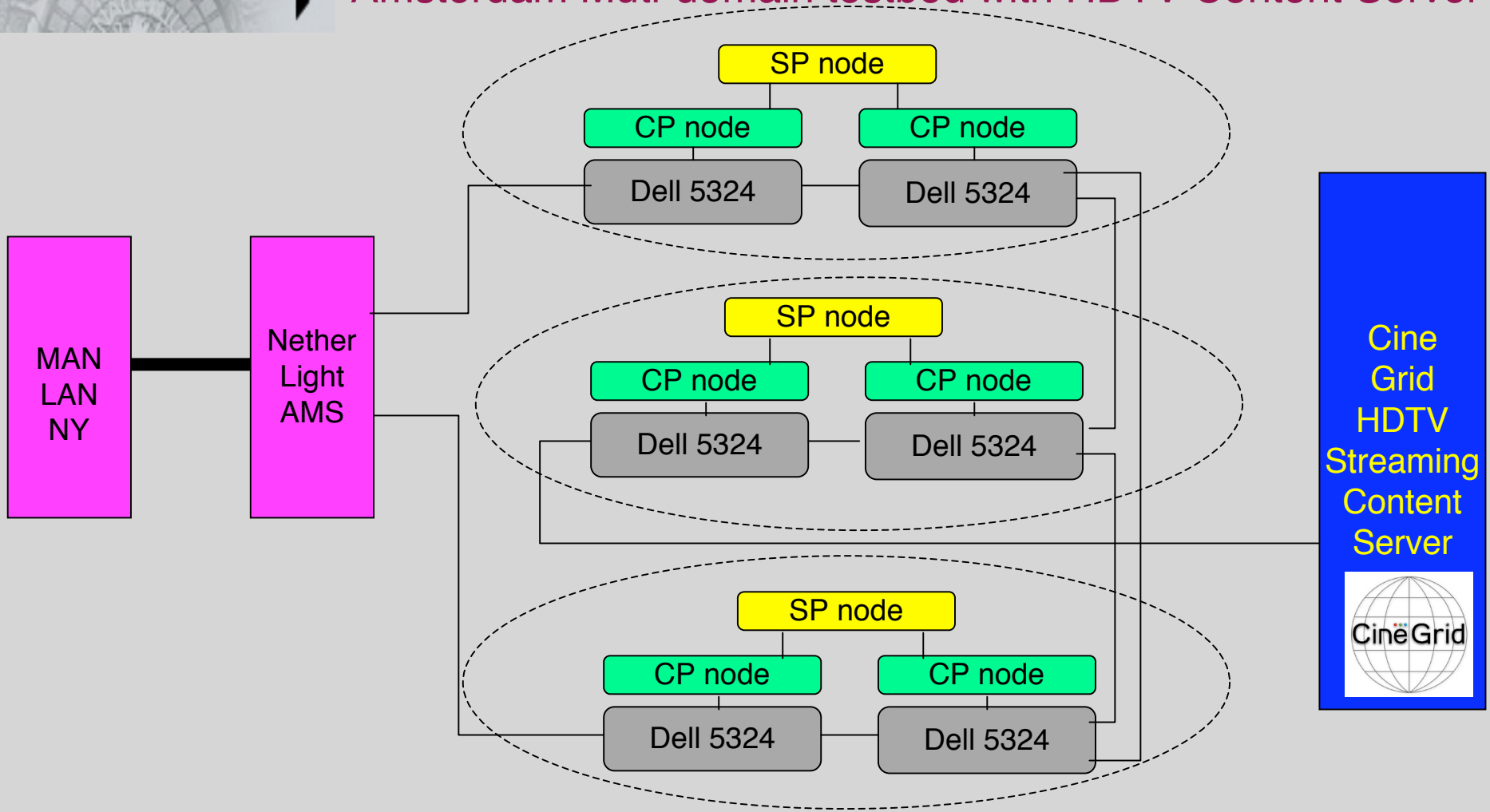
- Attracted serious attention from several communities
- Reached agreement with Internet2 to pursue the token idea's further for multi-domain access.
- Had very productive meetings where we decided:

1. Integrate both testbeds with transatlantic connection.
2. Use a common a GMPLS implementation (DRAGON) and integrate into token support into DRAGON release.
3. Integrate AAA with ESNET domain controller (OSCARS) to create multi-domain scenarios
4. Work together at WSDL describing Domain controller WS based interface for both East-West & Northbound functions
5. Work together at SC 07 demo showing multi-domain ease of use to both scientist and networking people.
6. Work together thereafter.
7. Integrate Phosphorus efforts (Nortel and SURFnet).

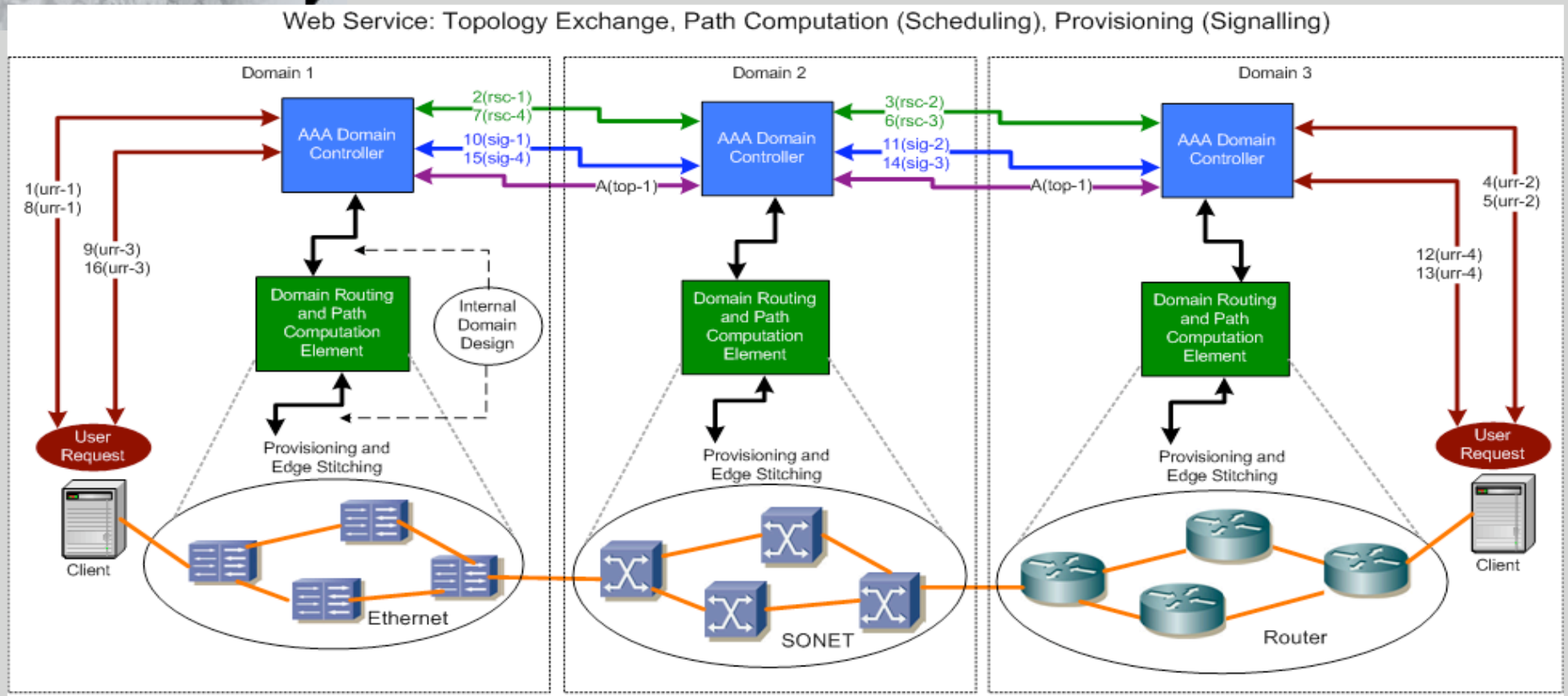
Multi-domain Token Based GMPLS setup for SC 07



Amsterdam Muti-domain testbed with HDTV Content Server



AAA role



User Request/Response
urr-1: startReservationRequest(Source, Destination, Bandwidth, Time, User Certificate),UserPathScheduleResponse
urr-2: RemoteUserReservationRequest, RemoteUserReservationResponse
urr-3: startPathSetupRequest, startPathSetupRequest
urr-4: RemoteUserPathSetupRequest,RemoteUserPathSetupResponse

Four XML Schemas and WSDL Services need to be defined:
Client Request/Response
Topology Exchange
Path Computationl(Scheduling)
Provisioning (Signaling)

Topology Exchange (XML Schema format Network Graph, Very Little Dynamic Information Exchanged)
top-1: getNetworkTopology

Resource Scheduling
rsc-1: getConfirmedPathRequest(Source, Destination, Bandwidth, Time, Domain1 Certificate, Path Computation Result (Loose Hop), Approval Indicated for Domain 1,vlan range indicated)
rsc-2: getConfirmedPathRequest(Source, Destination, Bandwidth, Time, Domain2 Certificate, Path Computation Result (Loose Hop), Approval Indicated for Domain 1,2, vlan range adjusted)
rsc-3: getConfirmedPathResponse(Confirmation Indicated for Domain 3, specific vlan selected)
rsc-4: getConfirmedPathResponse(Confirmation Indicated for Domain 2 and Domain 3) ("confirmed loose hop explicit route object" now available, includes identification of a "confirmed" vlan)

old

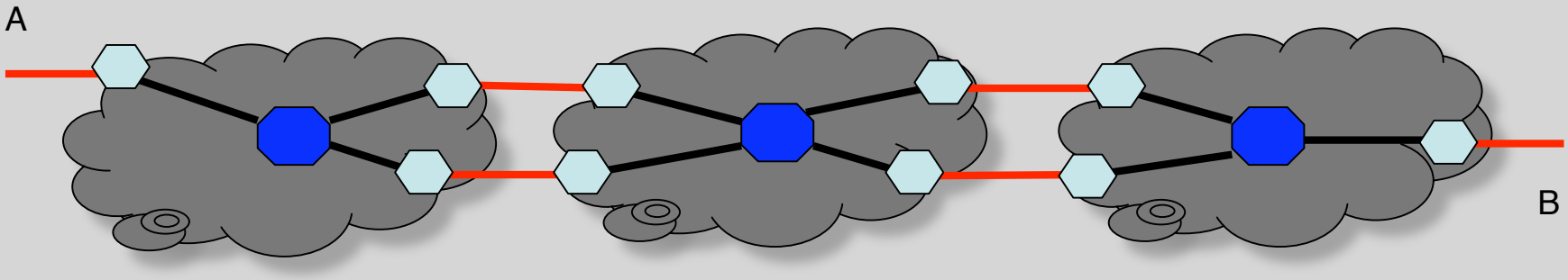
Signaling
sig-1: createPathRequest (PathID, Domain1 Certificate, Approval Indicated for Domain 1)
sig-2: createPathRequest (PathID, Domain2 Certificate, PathDetails(Confirmed Loose Hop ERO), Approval Indicated for Domain 1,2)
sig-3: creatPathResponse (PathID, Domain3 Certificate, PathDetails (Confirmed Loose Hop ERO), Approval Indicated for Domain 3)
sig-4: createPathResponse (PathID, Domain2 Certificate, PathDetails (Confirmed Loose Hop ERO), Approval Indicated for Domain 2,3)

In short you have 4 phases

- **Request path** – by user / grid middleware / application etc.
- **Find candidate path**: Topology exchange
- **Schedule / negotiate path** (compute optimal)
- **Use**: signal / provision

Where do the Tokens fit ?

Path Request and subsequent path finding / reservation process negotiates with each domain to obtain a specific path, but

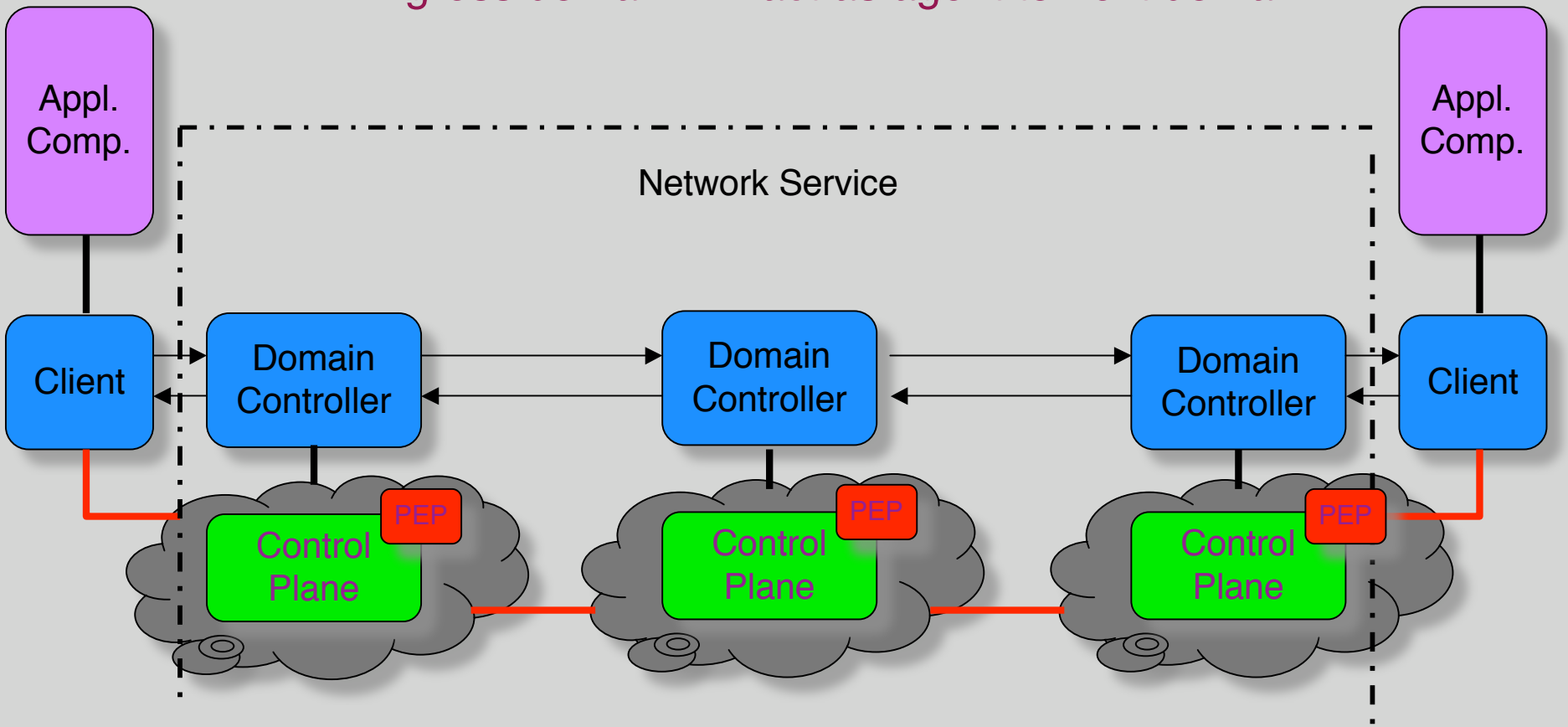


Who will ask the relevant questions to whom ?

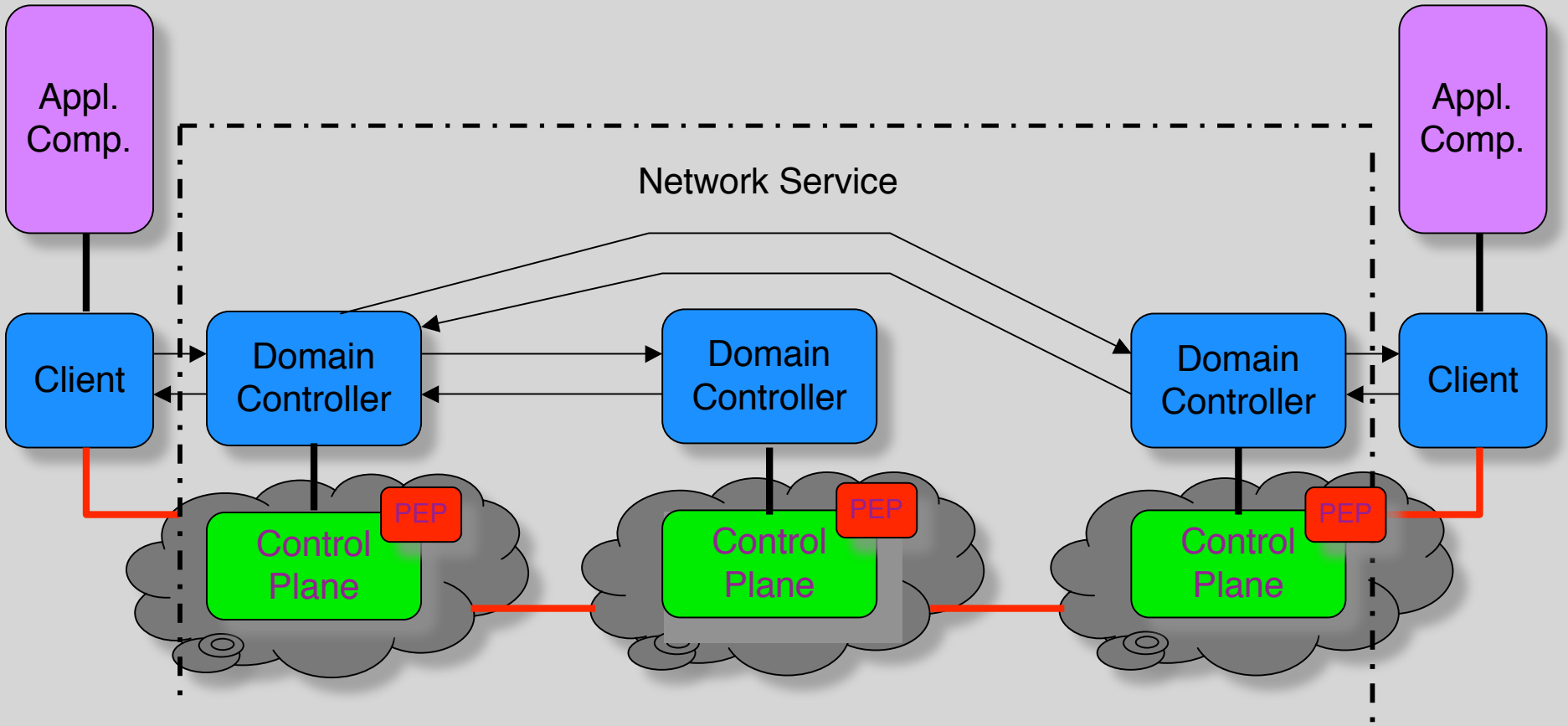
Two styles: ***Service Provider-*** and ***Grid- approach***

First style has two sub-approaches.

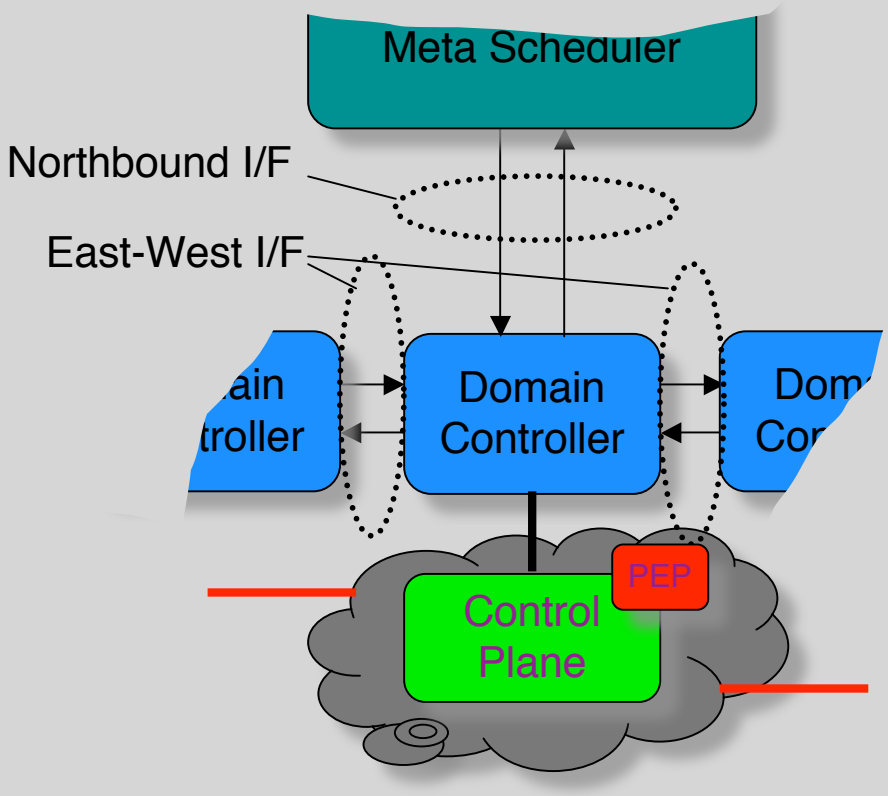
1a. The Service Provider approach using ***chained signaling***
- ingress domain will act as agent to next domain



1b. Service Provider approach with ***tree signaling***

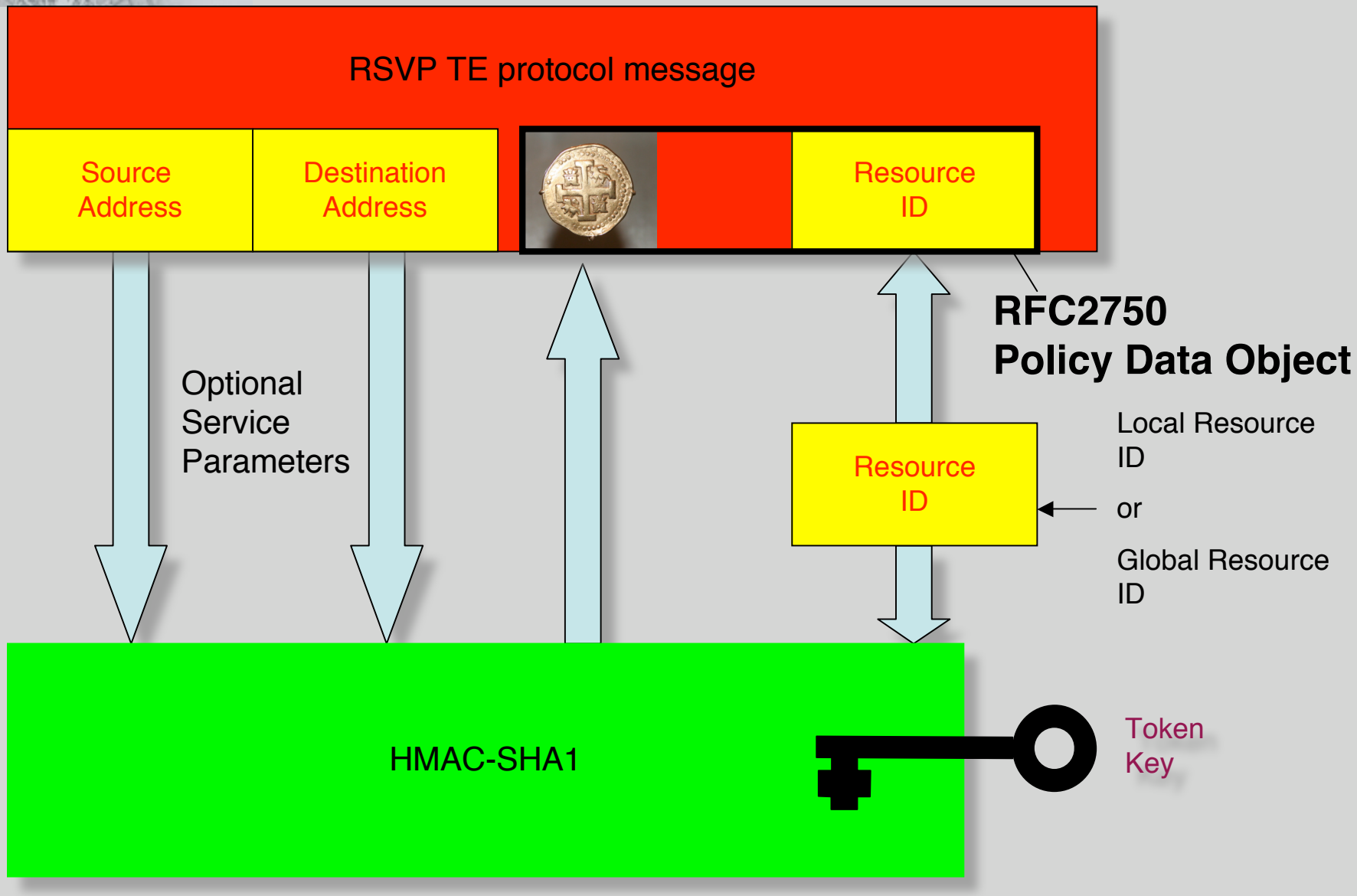


Goal Domain Controller UNI: support both **chain and tree**

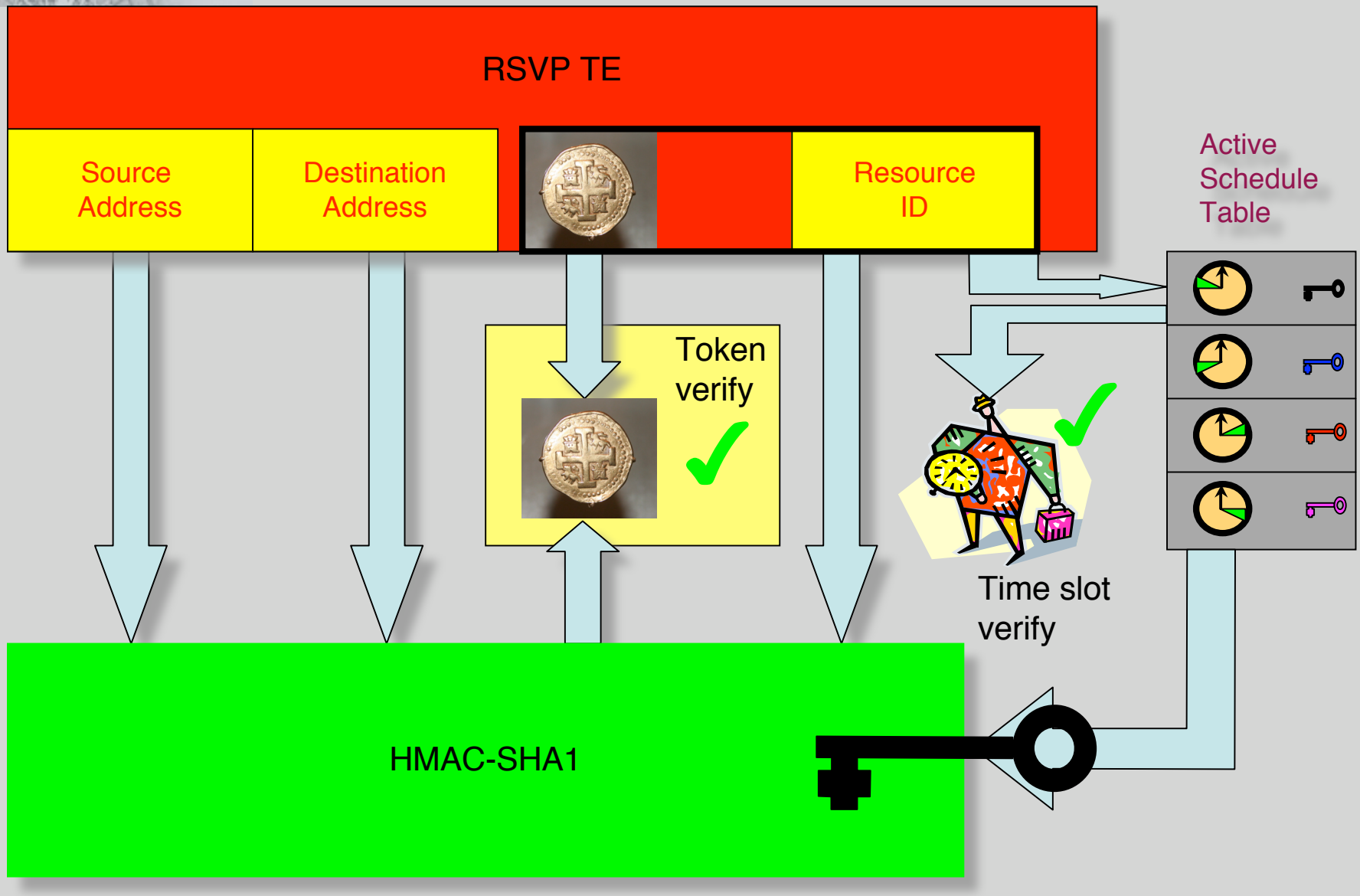


With Internet2 we came last Januari to the conclusion that In essence several types of questions asked via the interfaces are similar: Can we combine the questions by specifying a single type of interface ?

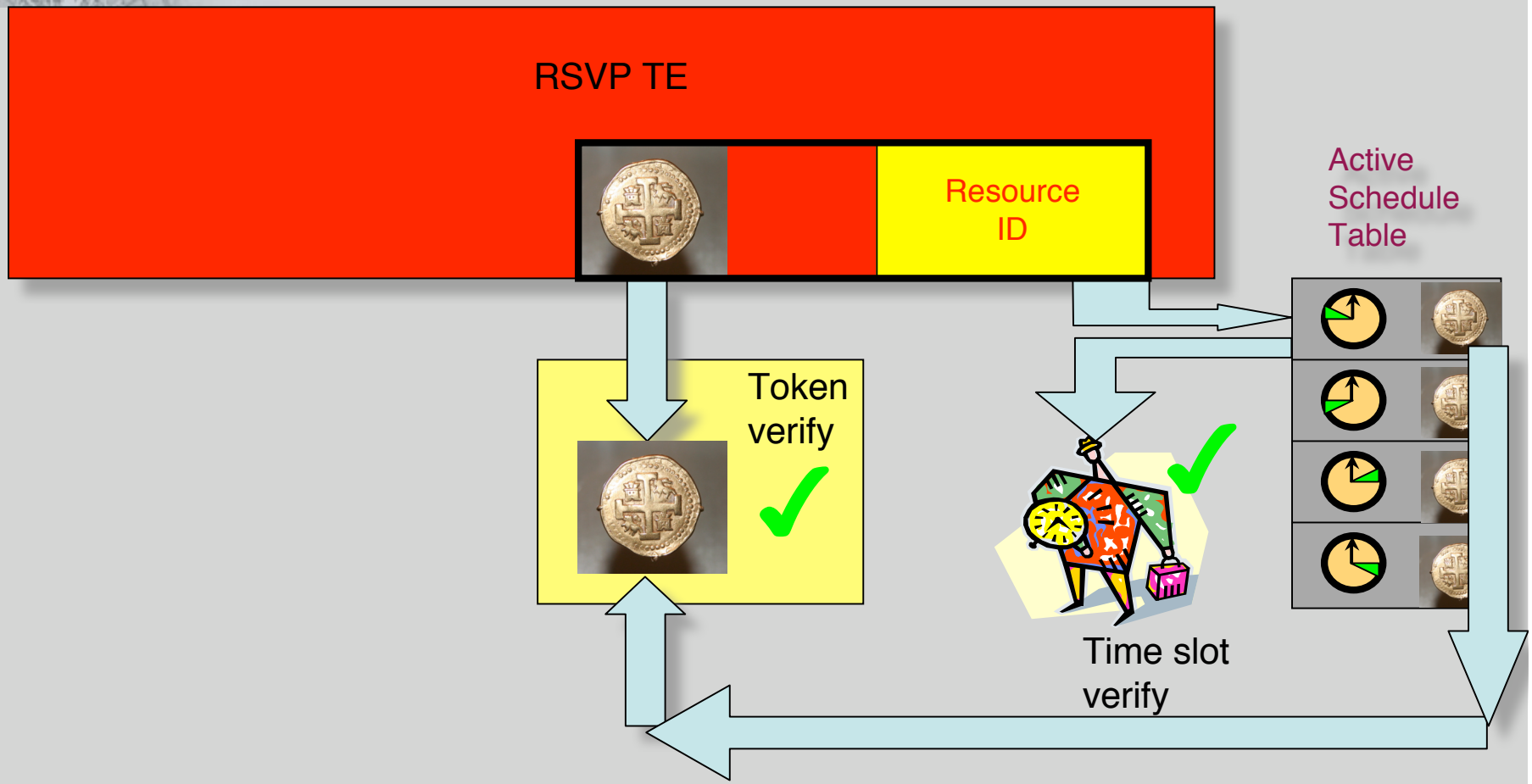
Token generation - detailed



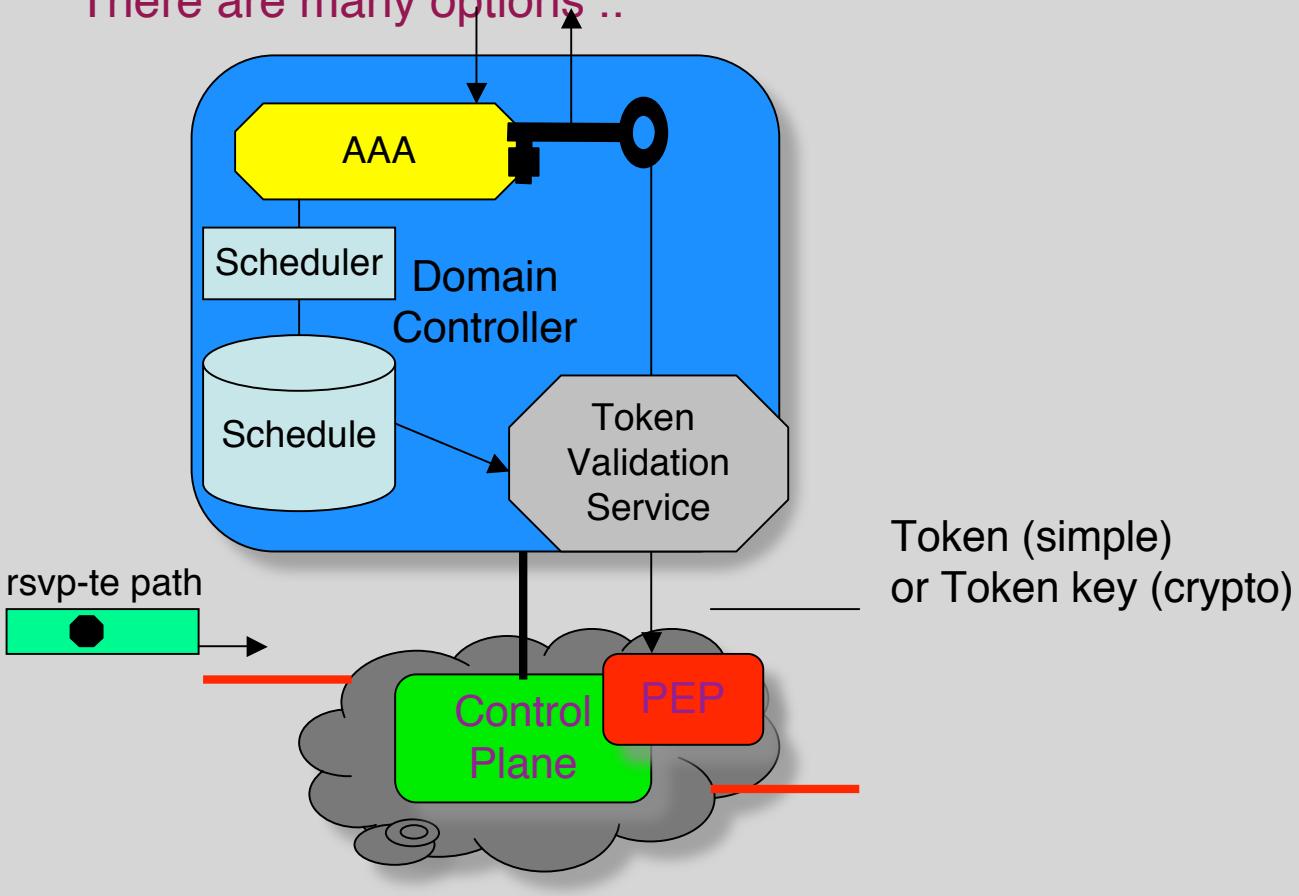
Token validation at Policy Enforcement Point - crypto based



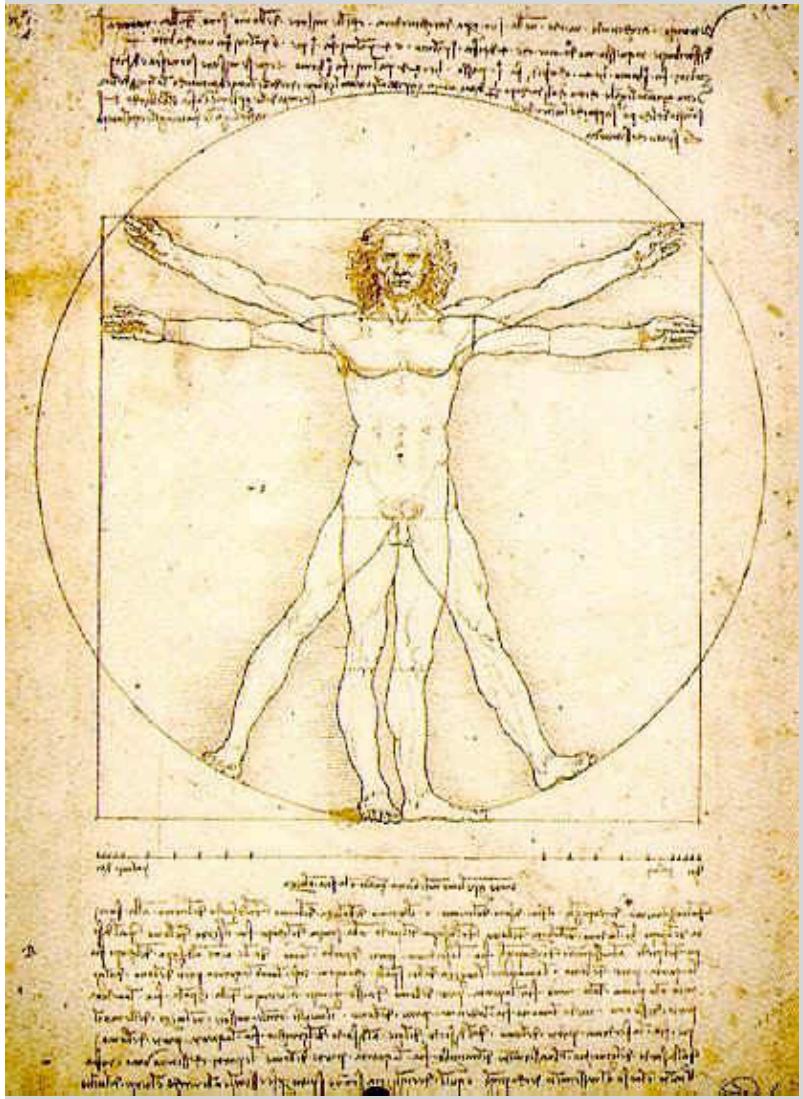
Token validation at Policy Enforcement Point - simple



Multi - domain case using GMPLS signaling:
Tree: Token key generation can be done within each domain to indicate commit of the service
Chain: Token key could be generated in last domain,
There are many options ..



Vitruvius - an architect 1st cent. BC working for Ceasar said:



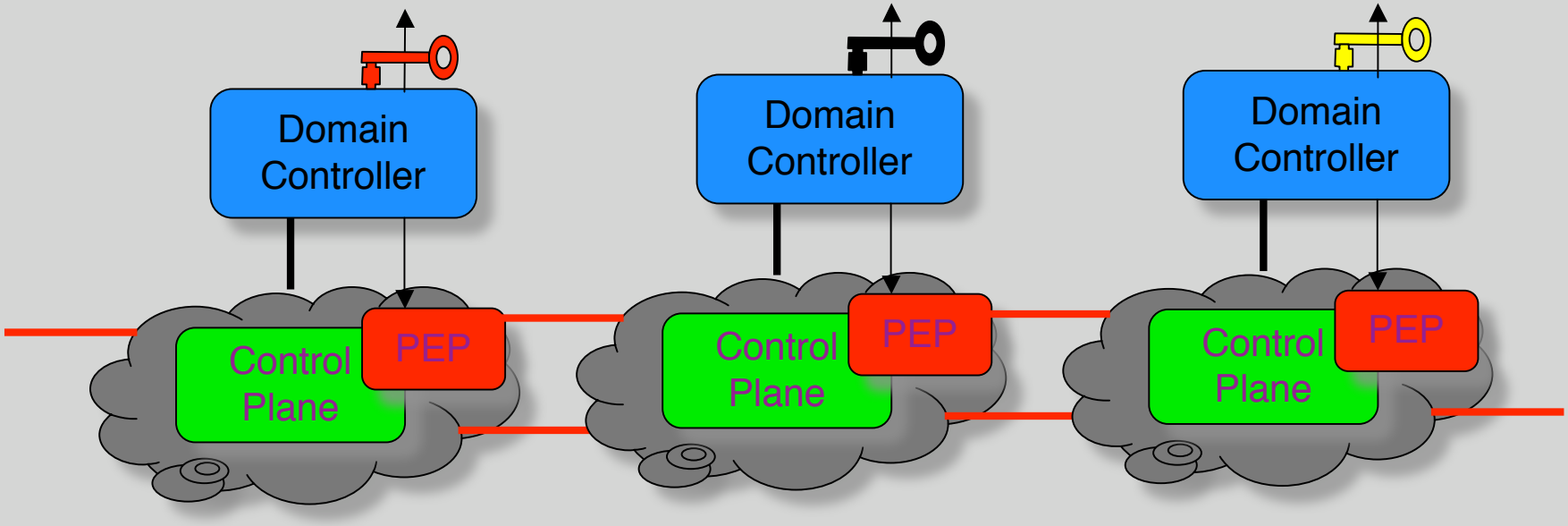
"Cum in omnibus enim rebus, tum maxime etiam in architectura haec duo insunt, quod significatur et quod significat."

Architect Joseph Gwilt (1826) translated this into:

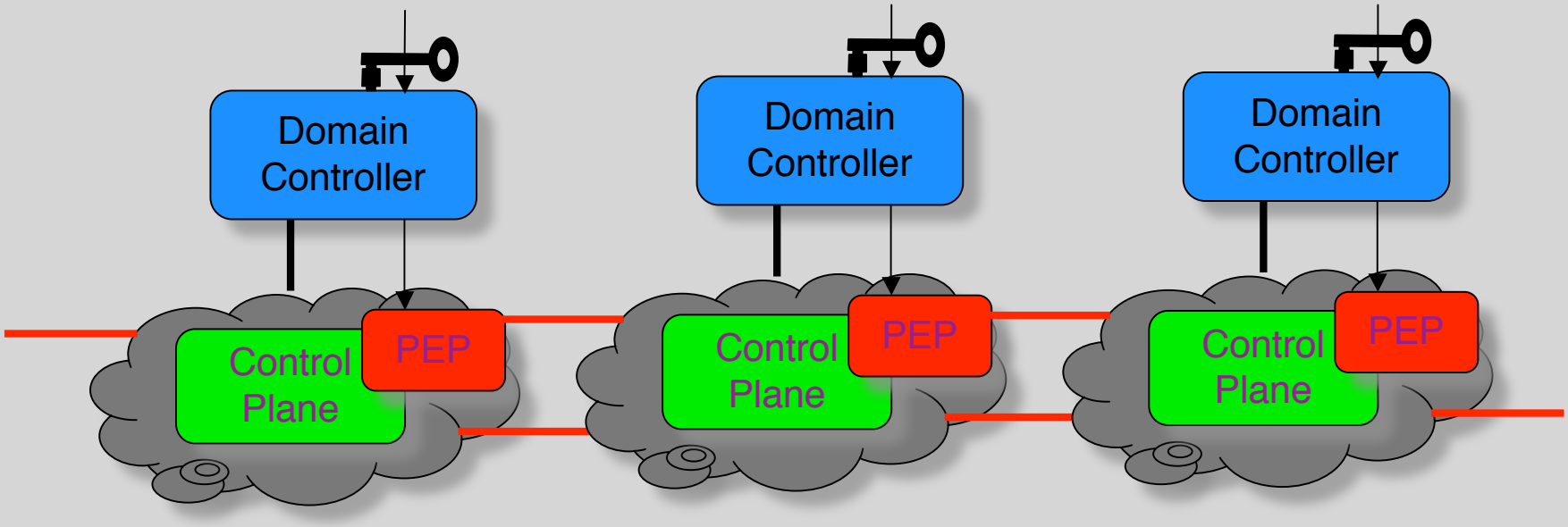
" For as in other arts, architecture must constantly keep in view the intention and the material used to express that intention"

Network building blocks should allow expression of as many intentions as feasible.

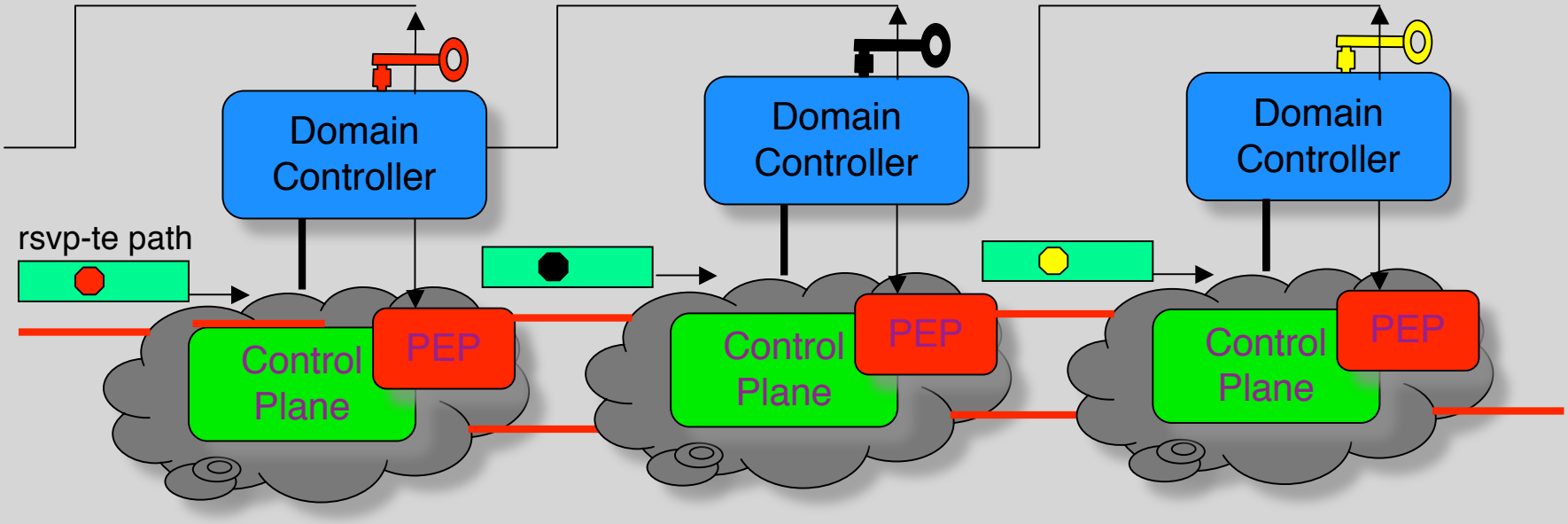
Token key generation: should each domain generate their own key or ...



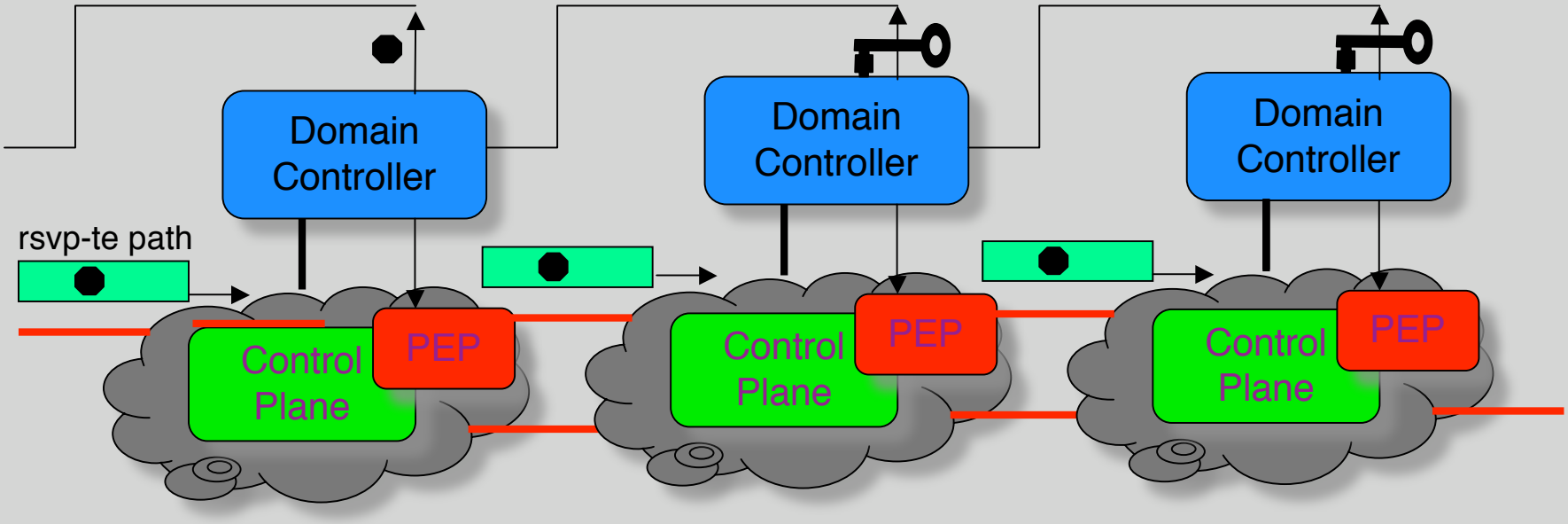
Be provisioned with the (same) key ....



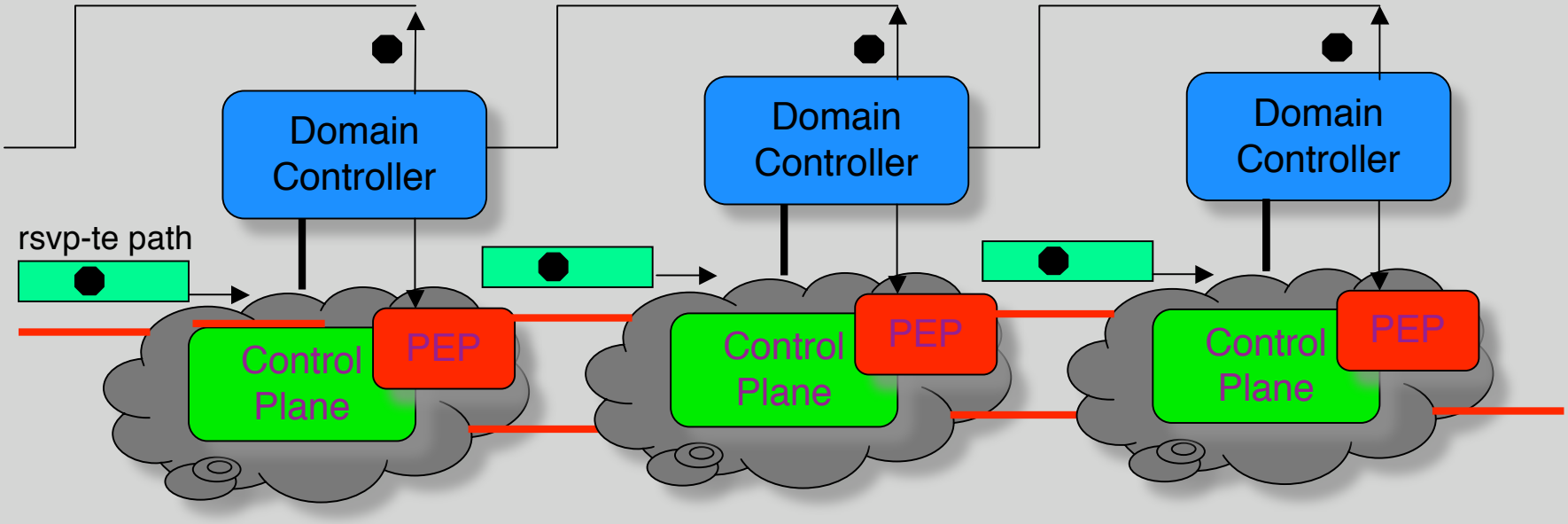
The upstream domain gets key from downstream domain.
Upstream domain regenerates token for downstream domain
Chain model style



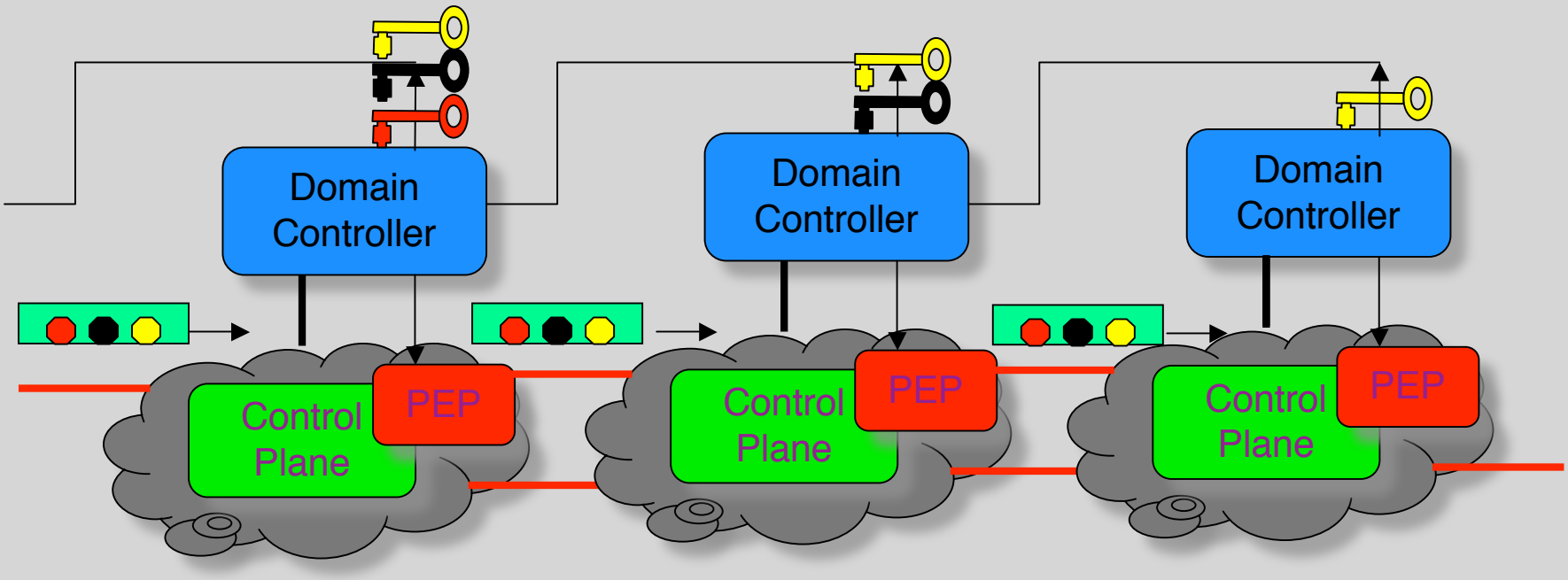
The upstream domain gets key from downstream domain. Last domain generates key, first domain the token to avoid Exchange key material with end user.



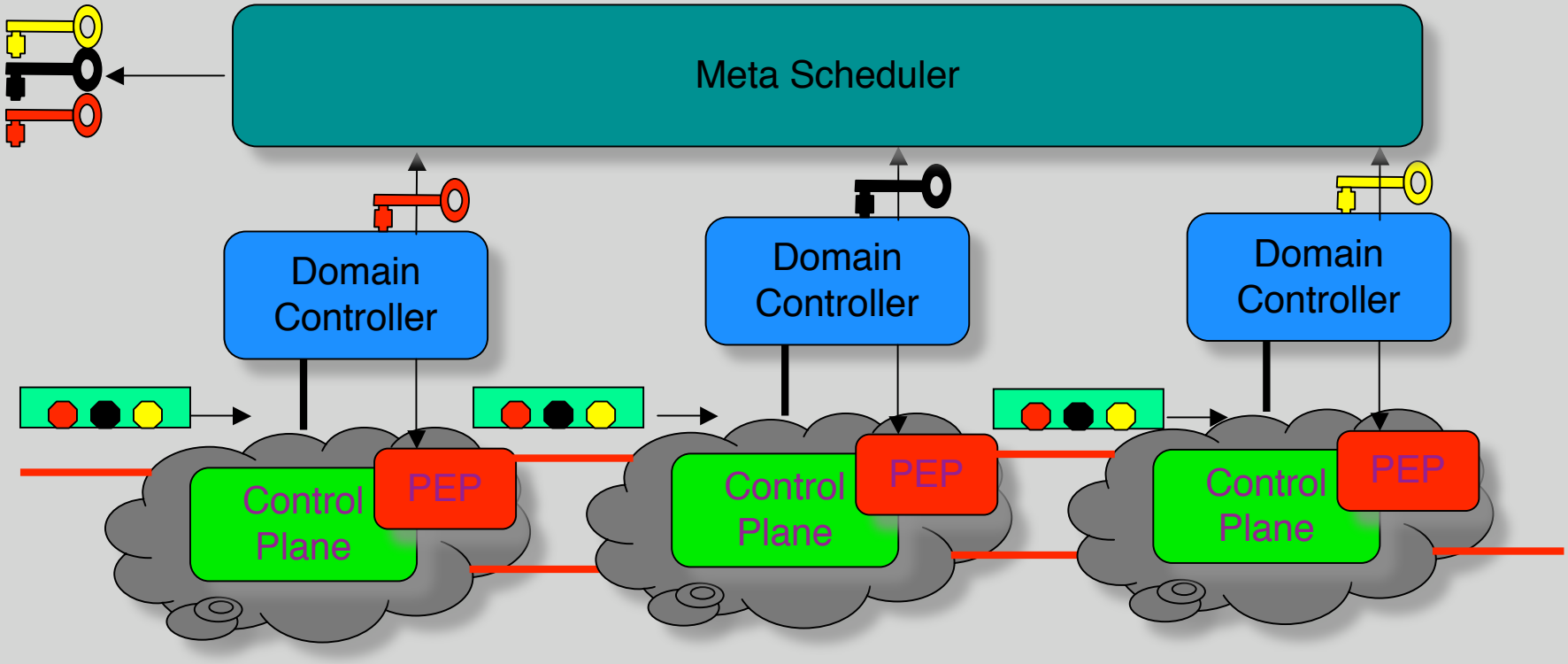
The upstream domain gets key from downstream domain.
Last domain generates key, first domain the token to avoid
Exchange key material with end user and other domains.
Current implementation with OSCARS/Internet2 IDC



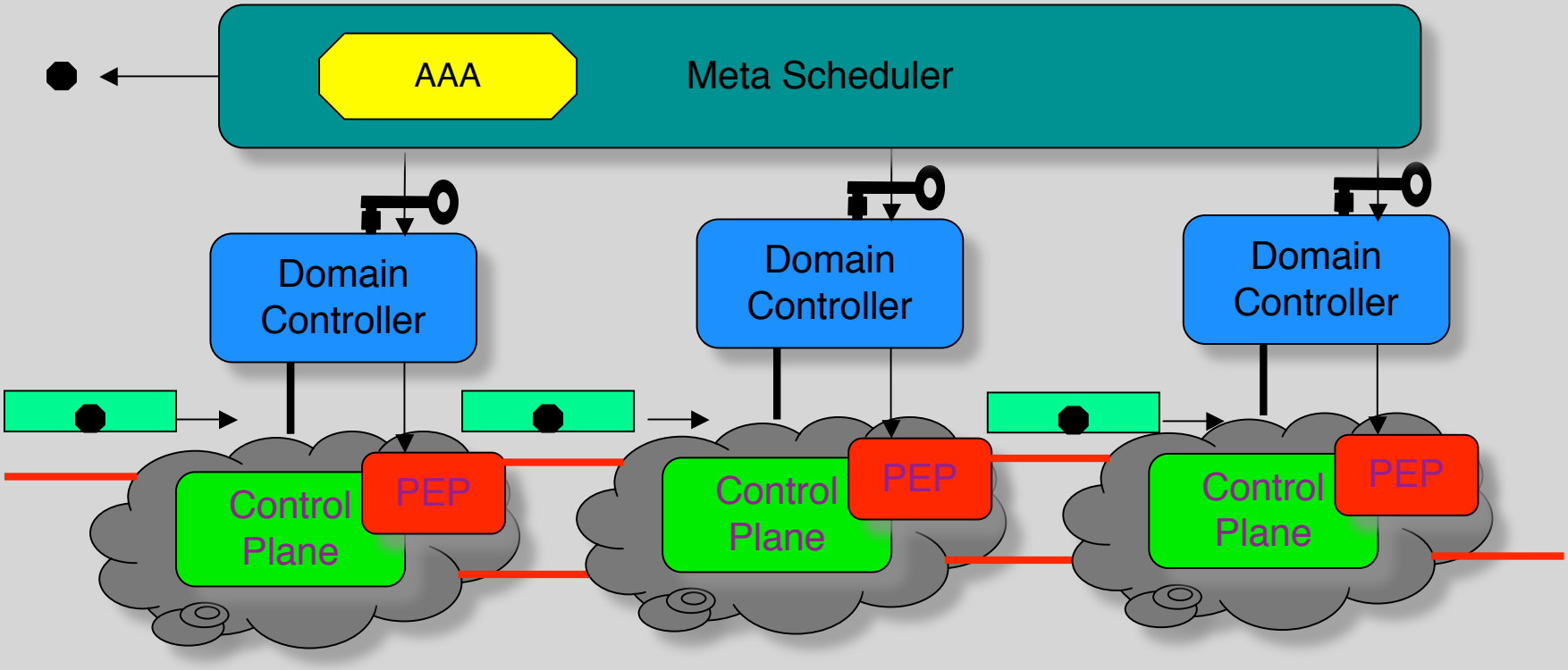
Source route fashion - every individual PEP recognizes its token



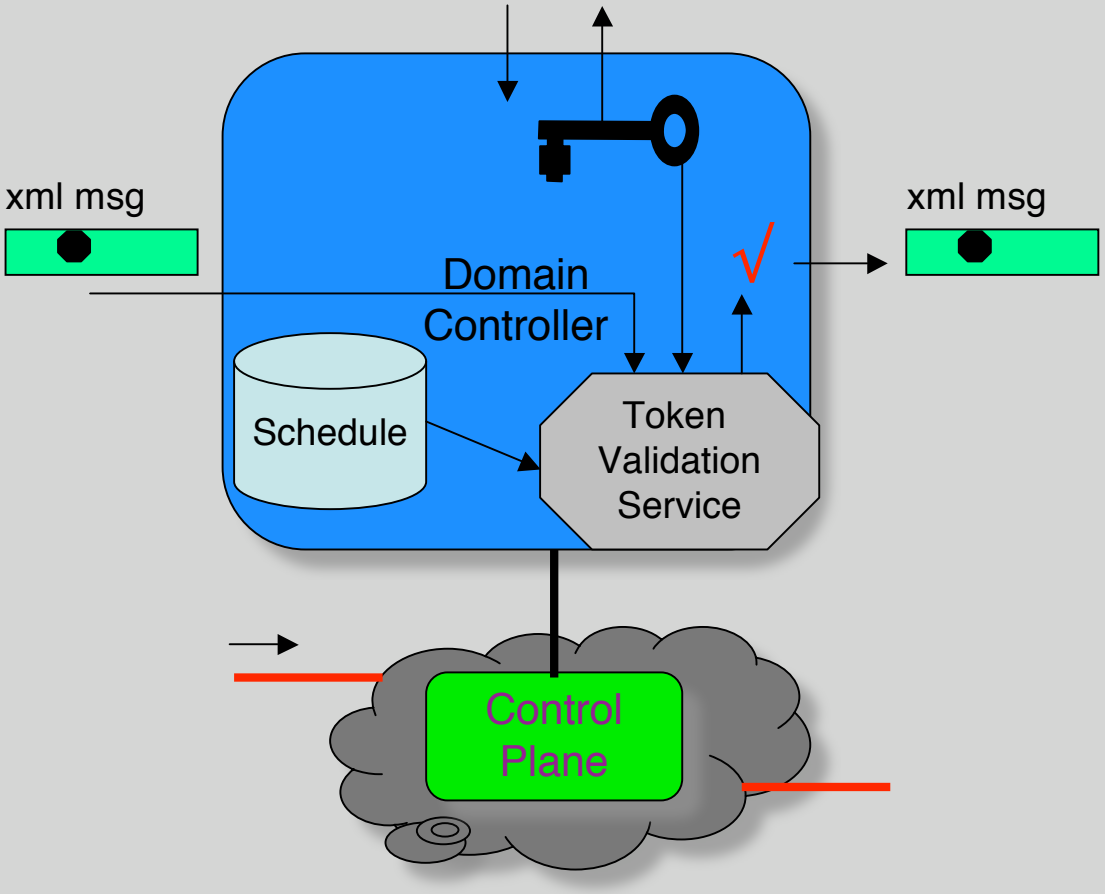
A meta-scheduler receives tokens from every domain and passes them on to job.



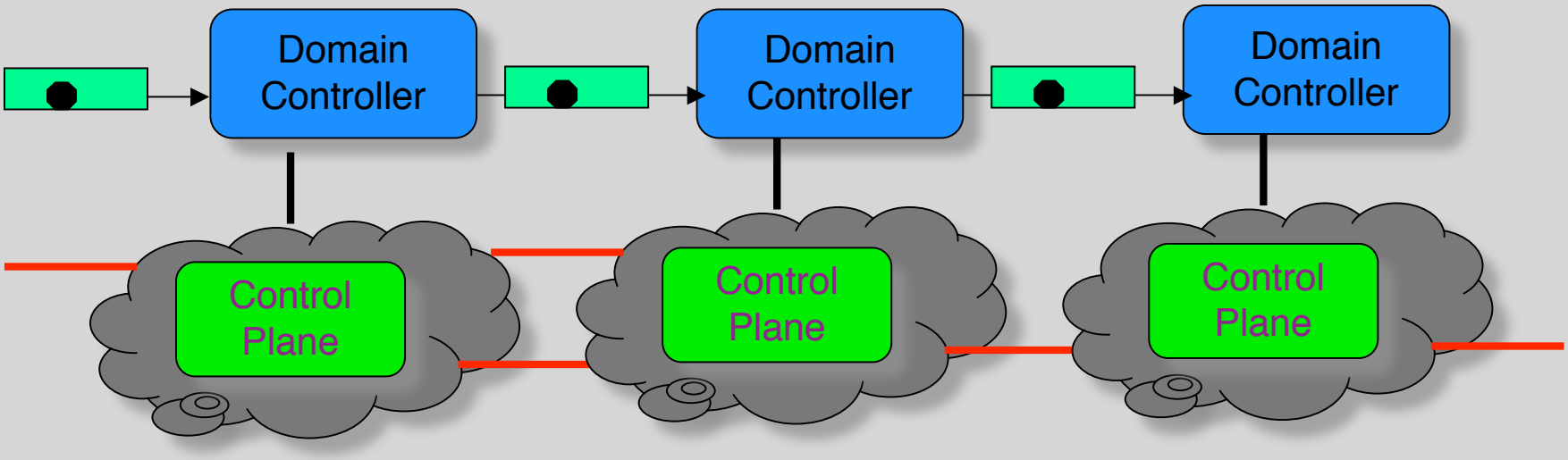
The meta-scheduler provisions domains with the same key
The alternative approach that will be shown at SC07
Intended to show the Phosporus - NextGrid approach.



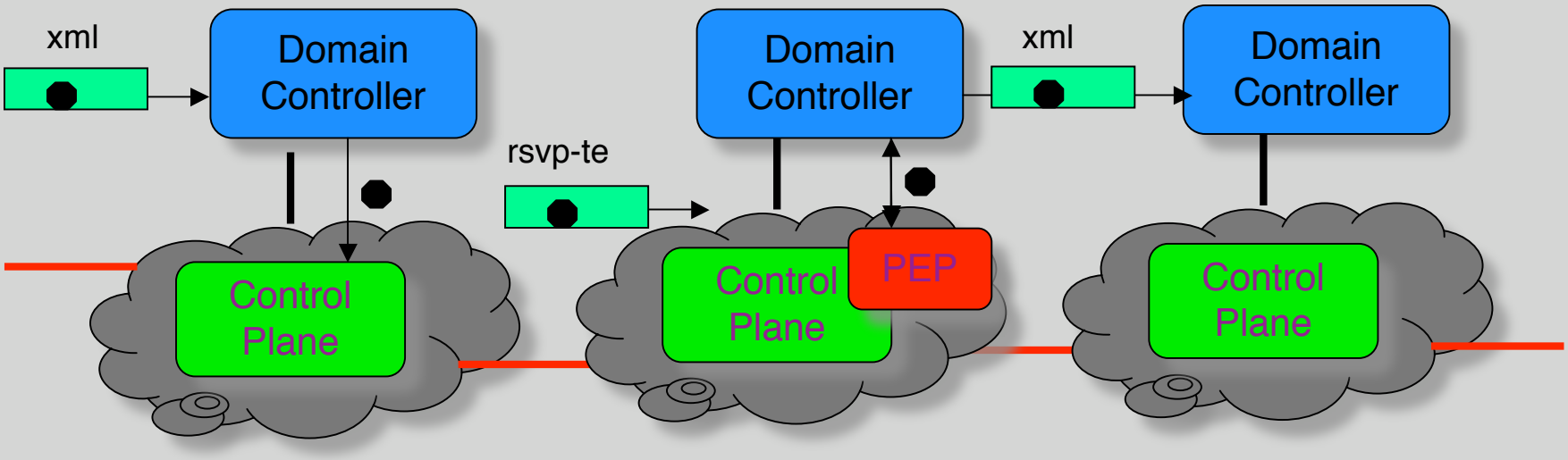
Use phase: Token signaling can also be done at IDC level using XML.



Multi-domain Token signaling at Inter Domain Controller level.

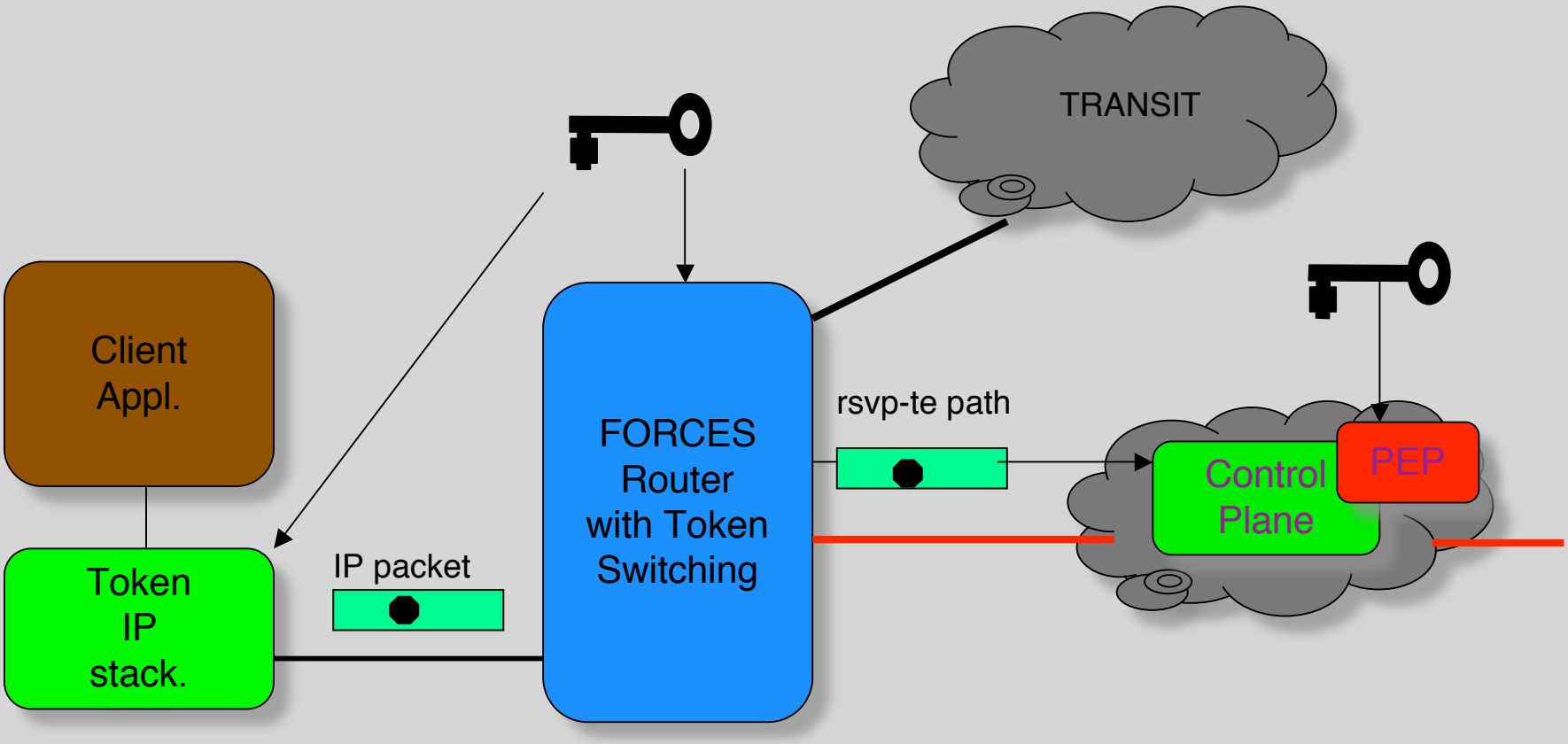


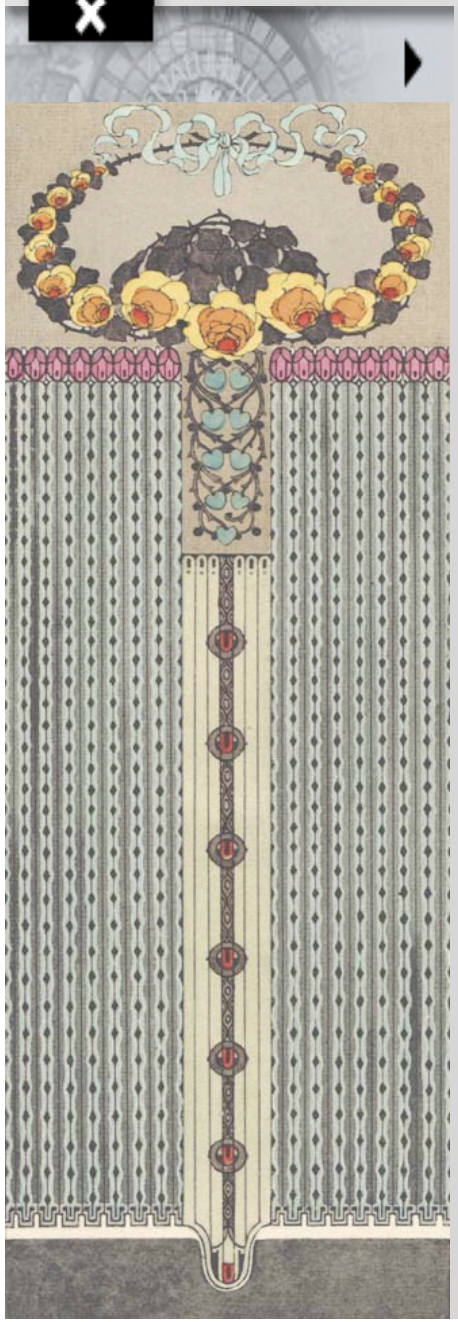
Hybrid Token signaling at Inter Domain Controller and GMPLS level.



Token based gateway router (part of Phosphorus)

Allows token marked IP packets to take GMPLS path,
Others are switched to the regular IP transit network





Objectives SC 07:

- Demonstrate the Token Validation Service integrated into OSCARS / DRAGON in collaboration with Internet2, SURFnet and Nortel.

Show:

1. The simplest of the multi domain GMPLS based token chain scenario's ie: last domain generates token and hands it to upstream domain – every domain compares the GMPLS RSVP TE contained token with the token that moved upstream.
2. CineGrid based HDTV (1gb/s) scenario using USB stick to carry the token from reservation to usage phase to show the decoupling of Authorization and Usage.
3. Also show the inter-domain interface which supports both **tree-** and **chain** style approaches
4. Show the FORCES based router as gateway between campus network and GMPLS network.

THANK YOU

LGOMMANS@SCIENCE.UVA.NL