PHOSPHORUS

Work Package 4
Authentication, Authorization and Accounting

Leon Gommans, Mihai Cristea, Yuri Demchenko
University of Amsterdam

Kick-off meeting Poznan October 17th

Overview

- Introduction
- What: Description of WP4 from technical annex
- How:
  - AAA concepts
  - AAA within GMPLS networks
  - AAA at network exchange points
  - Two presentations on some implementation details

Introduction

- **A**uthentication: Who are you ?
- **A**uthorization: What are you allowed to do ?
- **A**ccounting: How much have you used ?
- Focus of projects is towards **authorization** assuming some form of authentication will be used.
- Demand and Supply side.
- Multiple Independent Suppliers,
- Demand side represented by multiple organizations
- Only if accounting is implemented, suppliers will want to collaborate.
- Accounting is second objective.
- AAA systems handle AAA requests and (policy based) decisions using some format. Focus is both on handling and message formats.

WP 4 Objectives PM 1 - 18

- **WP4 (Service Plane - AAA)** will focus on implementing and integrating Authentication, Authorization and Accounting solutions for the PHOSPHORUS test-bed. The objectives of WP4 in the first 18 month are:
  1. To study the applicability of current and emerging AAA related technologies in order to select a suitable set with enough flexibility to create and test the interoperability of optical network domains. Collaborations with GÉANT2 (JRA5), DRAGON and EGEE will be established which and will be used as a base.
  2. Collaborate with WP1, 2 and 3 to establish their specific needs towards AAA and describe their needs in a uniform way that allowing a more generalized implementation
  3. To create prototypes, running in a test bed, which demonstrates authorization sequences applied in multiple functional layers of the network. The AAI work within GÉANT2 and VOMS work within EGEE will be used as starting point and expanded.

- Consequently the work is organised into
  - Task 4.1 AAA architecture selection
  - Task 4.2 AAA scenario development
  - Task 4.3 Integration and testing

Task 4.1 AAA Architecture Selection

Work of relevant network standards bodies (IETF, GGF, TGC, OIF, ITU-T, IEEE), European or national Grid projects (EGEE, Globus, Unicore, etc.) and optical networking projects (GアNT2, GLIF, VIOLA) will be considered and their architectures will be briefly described and classified. This work will be used to position AAA technologies such that selections can be made to create interoperable scenarios between optical network domains in the test-bed.

Activity 4.1.1 - Consider standard bodies based AAA architectures

Activity 4.1.2 - Consider Grid projects based AAA architectures

Activity 4.1.3 - Consider optical networking projects AAA and AAI architectures

Activity 4.1.4 - Selection of AAA architectures for test-bed.

Task 4.2 AAA scenarios

RFC2904 and GFD.38 provide sequence models that describe an authorization process. This task will work with WPs 1,2 and 3 to describe AAA scenarios used within their WP by using the standards documents as a guideline. This WP will subsequently work on creating a number of different test scenarios involving available solutions and experiences from the implementations in the test-bed. The work is aimed at testing a set of AAA mechanisms capable of unifying the AAA process across multiple domains using different solutions. AAA/AAI mechanisms used within GÉANT2 (JRA5), gLite (EGEE) and Globus GT4 will be considered. Experience with these scenarios will help to identify advantages and disadvantages of particular approaches. It will also identify missing functionality. Performance, manageability, scalability are important considerations. Reporting will be done in D4.2.

- ***Activity 4.2.1 - Interact with WP1 and create AAA scenario.***

  This activity will study WP1 to identify AAA sequences interacting within- or with an NRPS.

- ***Activity 4.2.2 - Interact with WP2 and create AAA scenario***

  identify AAA sequences interacting within the GMPLS control plane or via the G-OUNI.

- ***Activity 4.2.3 - Interact with WP3 and create AAA scenario.***

  identify AAA sequences within Grid Application scenarios or via the G-OUNI.

- ***Activity 4.2.4 - Create ForCES based token based scenario.***

  the deployment of the RFC2904 token sequence in networking deployed within the IETF ForCES framework.

- ***Activity 4.2.5 - Create AAA scenarios for test bed.***

Task 4.3 Integration and testing

This task will integrate the selected AAA technologies into a test bed and perform experiments in collaboration with WP6. Test scenarios will be determined in collaboration with WP 1, 2 and 3 by task 4.2. This task will execute the defined tests and report results. This work will specify the required facilities in collaboration with WP6. This work will focus on creating inter-domain AAA scenarios as preparation to a (pre-)production network such as GÉANT2, to be considered in the second phase of this project.

- ***Activity 4.3.1 - Integrate selected AAA mechanisms in test bed***

  This activity will technically implement the AAA mechanisms selected in task 4.1

- ***Activity 4.3.2 - Create technical implementation plans for test scenario's***

  This activity will technically implement the test scenarios defined in task 4.2.

- ***Activity 4.3.3 - Perform test scenarios***

  This activity will perform the test scenarios and report the results in D4.2.

WP 4 Milestones PM 1-18

- **M4.1 – AAA architectures to be described are identified and selected (M6)**
  - This activity will consider protocols, languages and mechanisms that are currently being used to implement authentication, authorization and account functions in a Grid context. From this set, a selection will be motivated to implement scenario's that will be coordinated with WP1/2 and 3. AAA scenario's will involve both the Service Plane, which interfaces with the control plane as well as consider scenario's that involve s the data-forwarding plane.
- **M4.2 – Selected test-bed scenarios are implemented (M12).**
  - The selected functions will be implemented in the tested, which can perform a number of identified scenario's.
- **M4.3 – Selected test-bed scenarios have been tested (M18).**
  - The selected scenario's have been tested such that the can be compared and evaluated in terms of performance, flexibility or scalability.

WP 4 Milestones PM 19 - 30

- **M4.4 - Study to integrate findings into larger deployment scenario (e.g. GÉANT2/GLIF) completed (M24)**
  - The scenario's from M4.3 will now be considered for implementation and integration into a larger test-bed using external networks such as GÉANT2 and the GLIF.
- **M4.5 - Selected large scale deployment scenario(s) have been tested (M30).**
  - The large scale scenario's have been tested and documented.

WP 4 Deliverables PM 1 - 18

- **D 4.1 AAA Architectures and scenario's for multi-domain optical networking.**

  Based on studies (both theoretical and from experienced gained in the test-bed) performed in Task 4.1 and collected input from WP1, 2 and 3 (Task 4.2) this deliverable will describe and motivate scenario's and designs that are expected to demonstrate interoperable use of AAA and AAI components for implementing multi-domain optical networking.

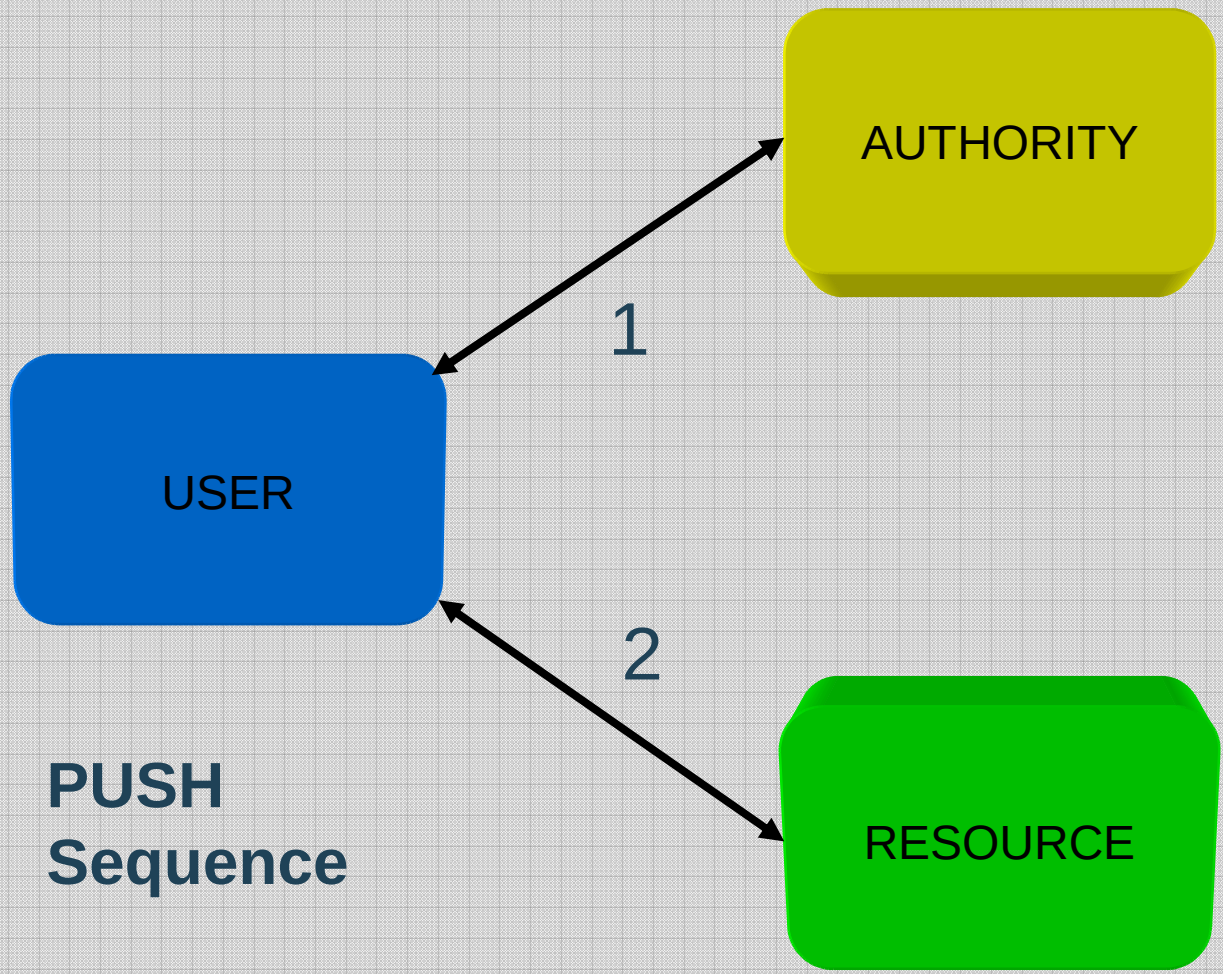
- **D 4.2 AAA scenario's and test-bed experiences.**

  Based on the motivated design and scenario's described in D4.1, this deliverable will describe the experiences gained from deploying AAA and AAI components in the test-bed to create an end-to-end lightpath across multiple domains.

WP 4 Partners + Personel

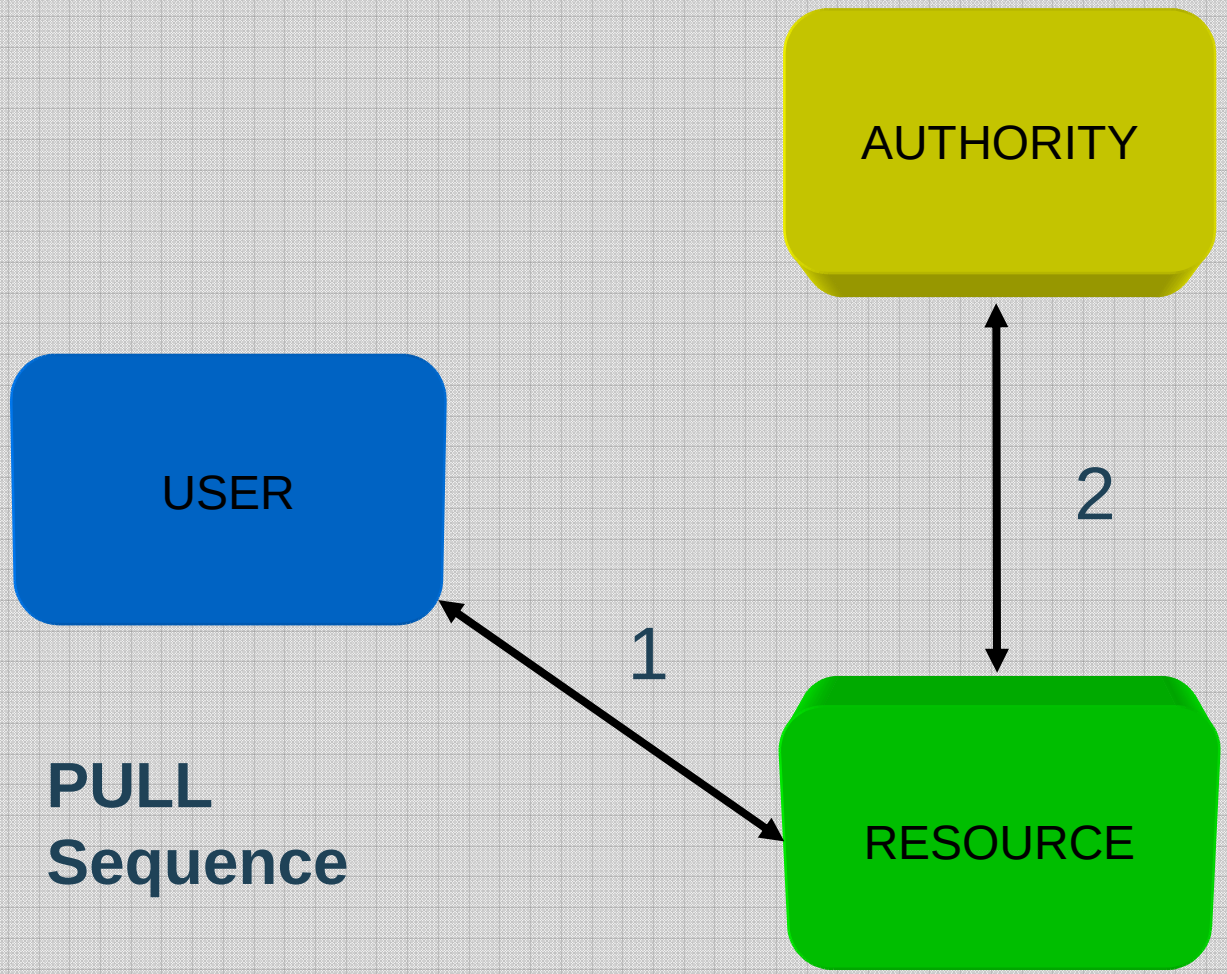
Task	Deliverables & Partners Contributions
Task 4.1	D4.1 UvA, FHG, University of Bonn.
Task 4.2	D4.2 UvA, HEL, CTI, NORTEL
Task 4.3	D4.2 UvA, HEL, CTI, NORTEL

AAA concepts: RFC 2904 Authorization sequences



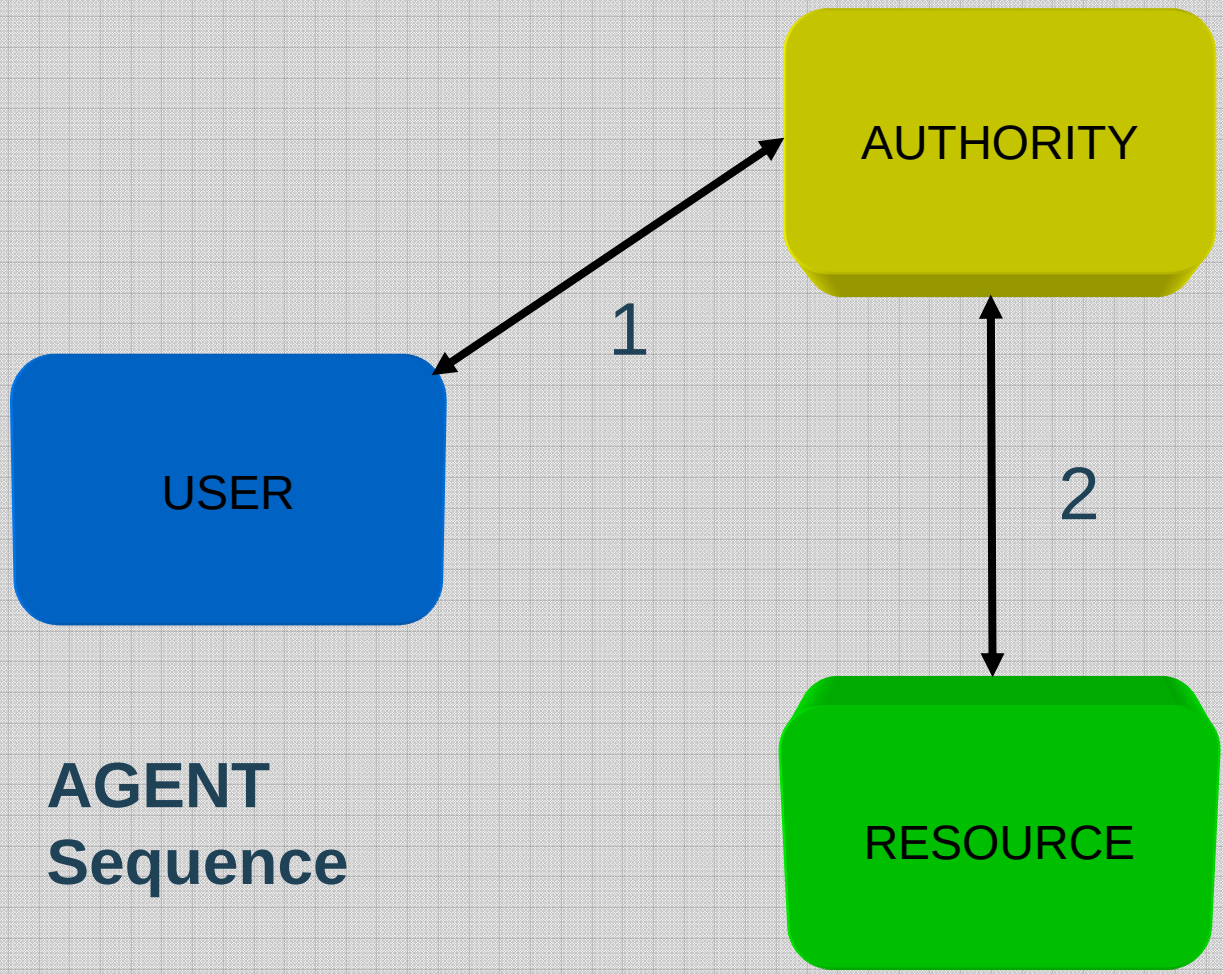
PUSH Sequence

AAA concepts: RFC 2904 Authorization sequences



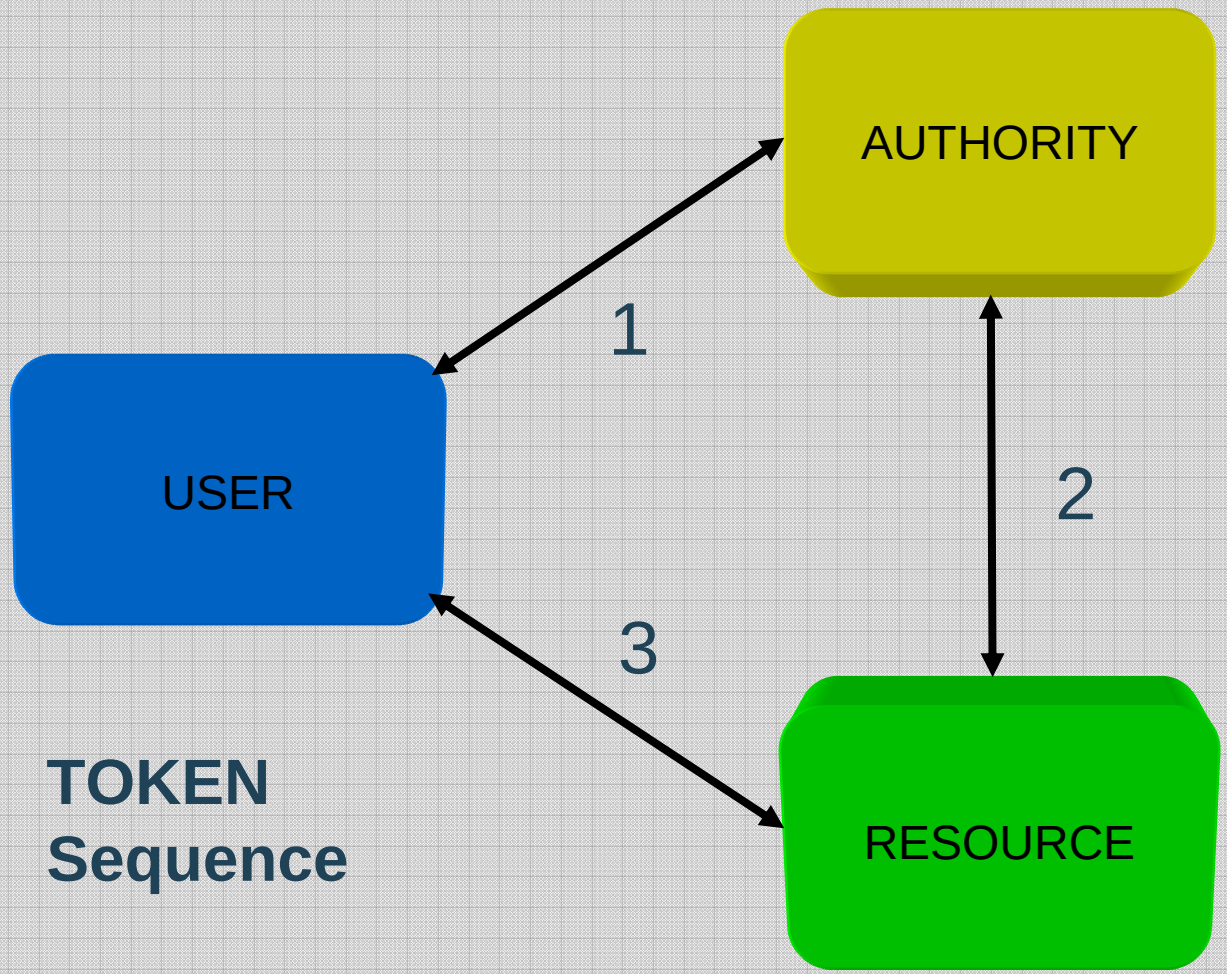
PULL Sequence

AAA concepts: RFC 2904 Authorization sequences

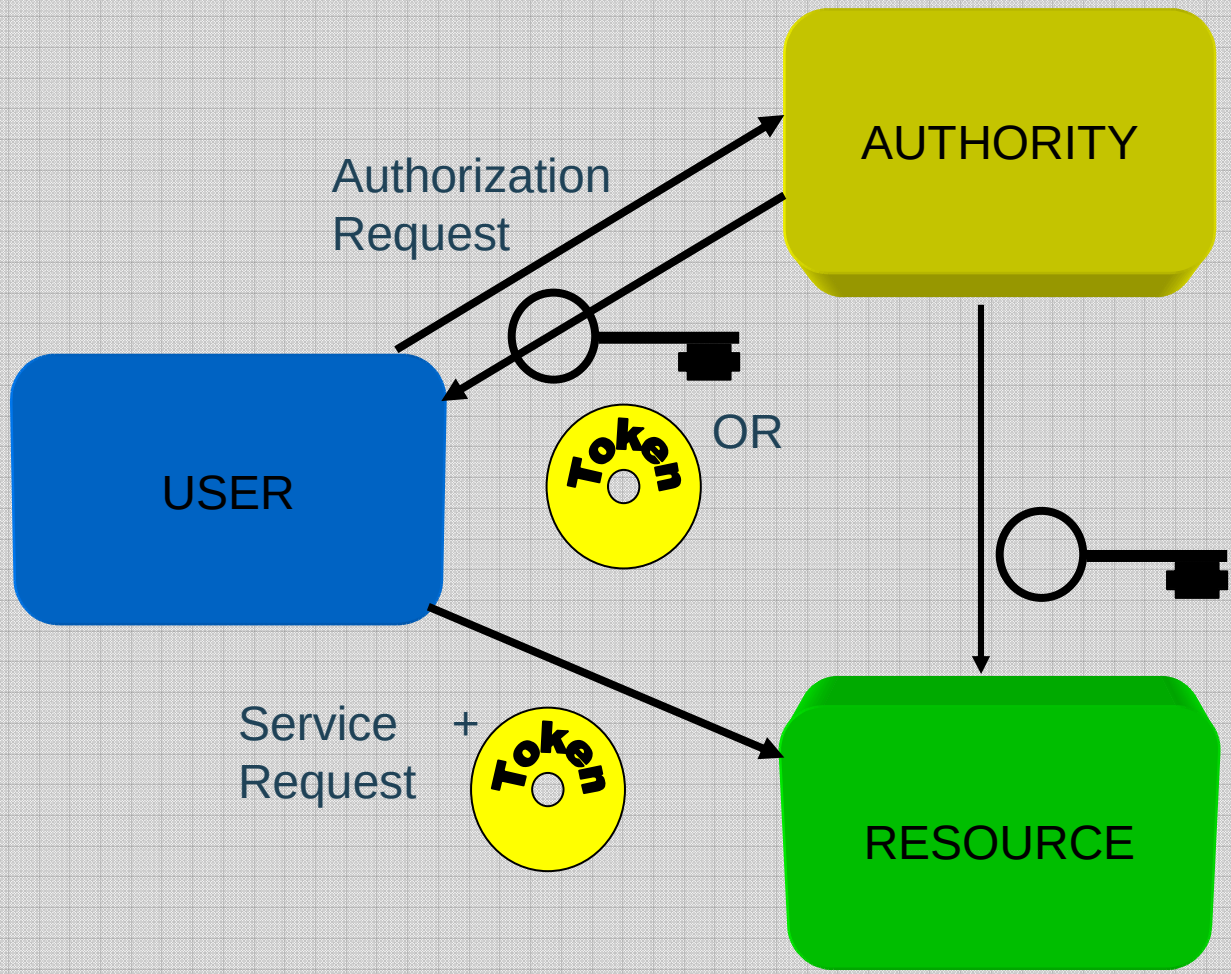


AGENT Sequence

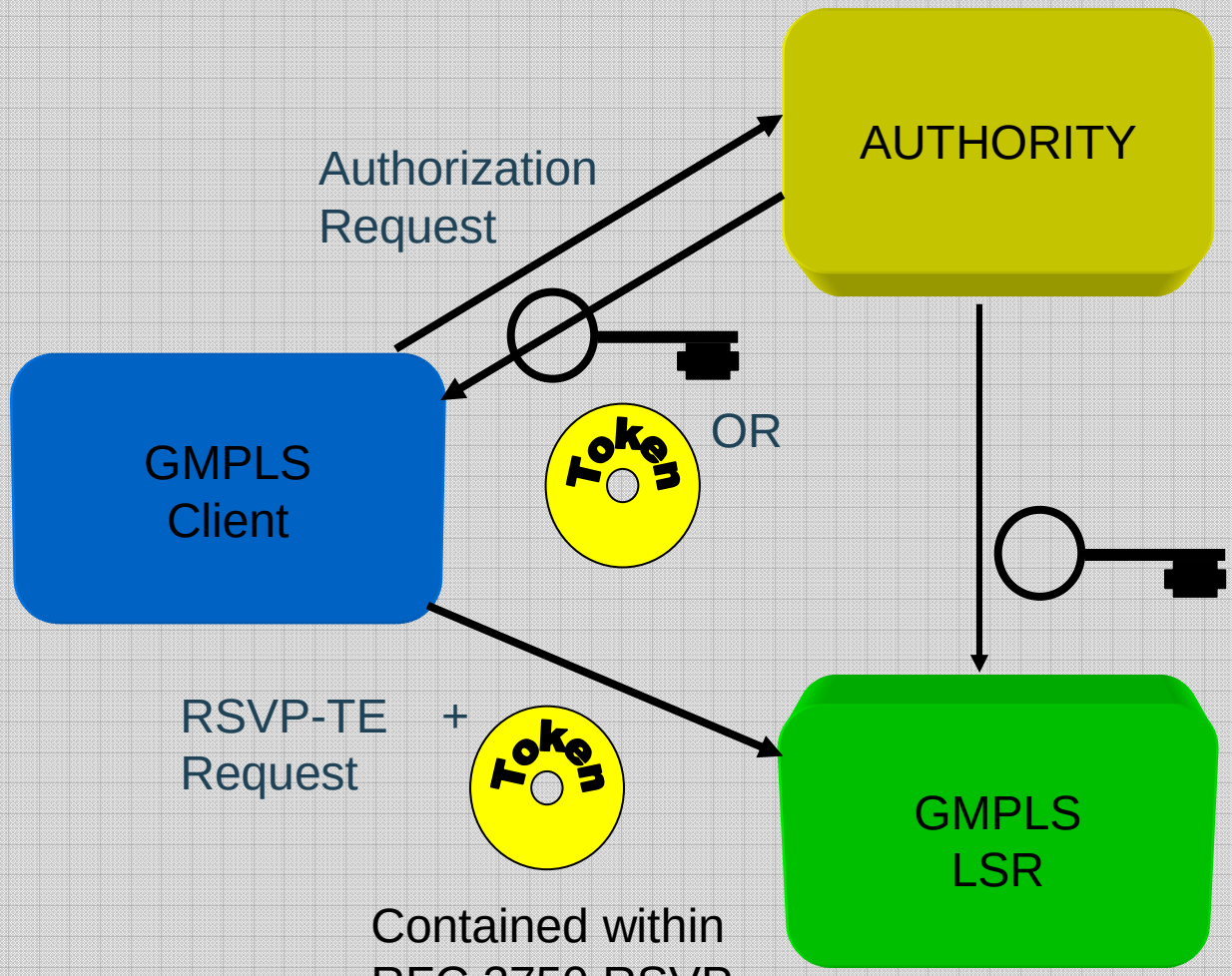
AAA concepts: Combination example



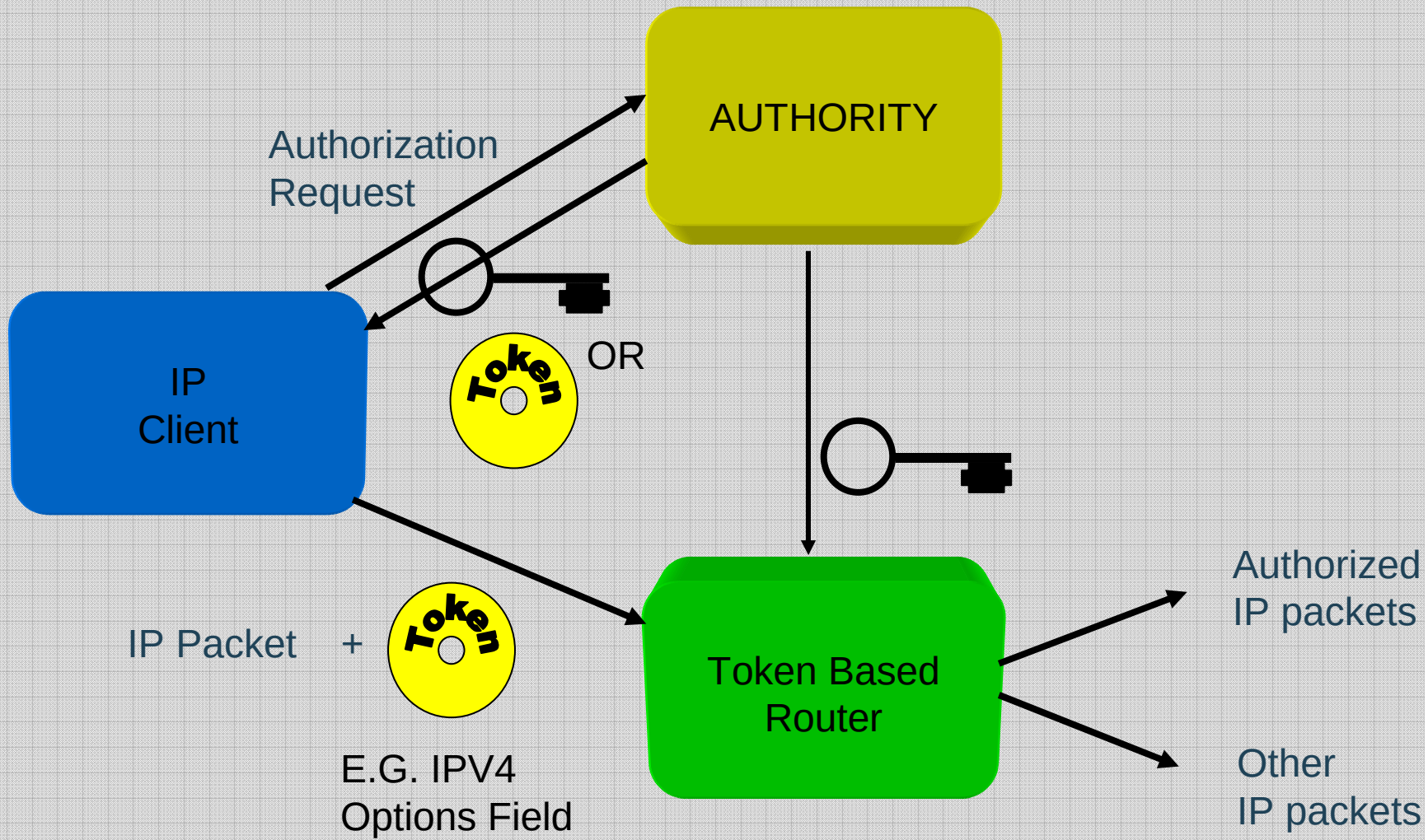
AAA concepts: Token Sequence in more detail



Tokens and GMPLS



Tokens inside IP packets

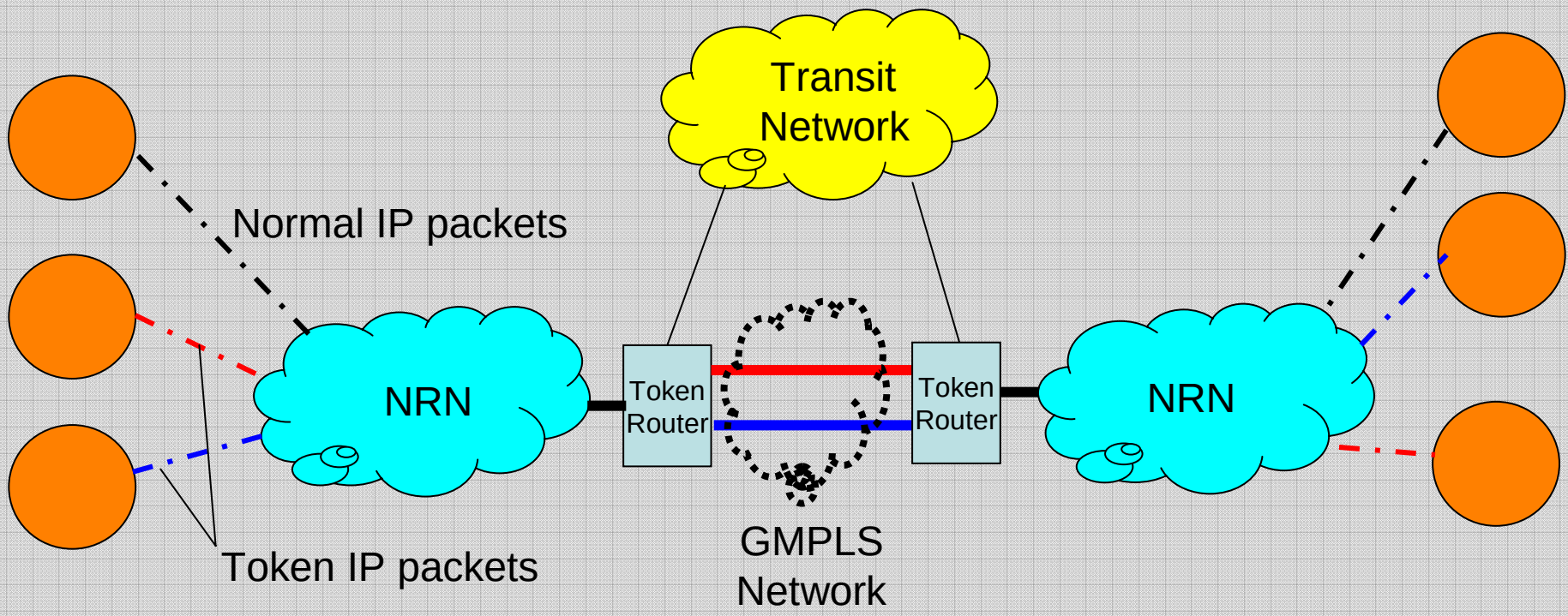


Which, What, Where and How

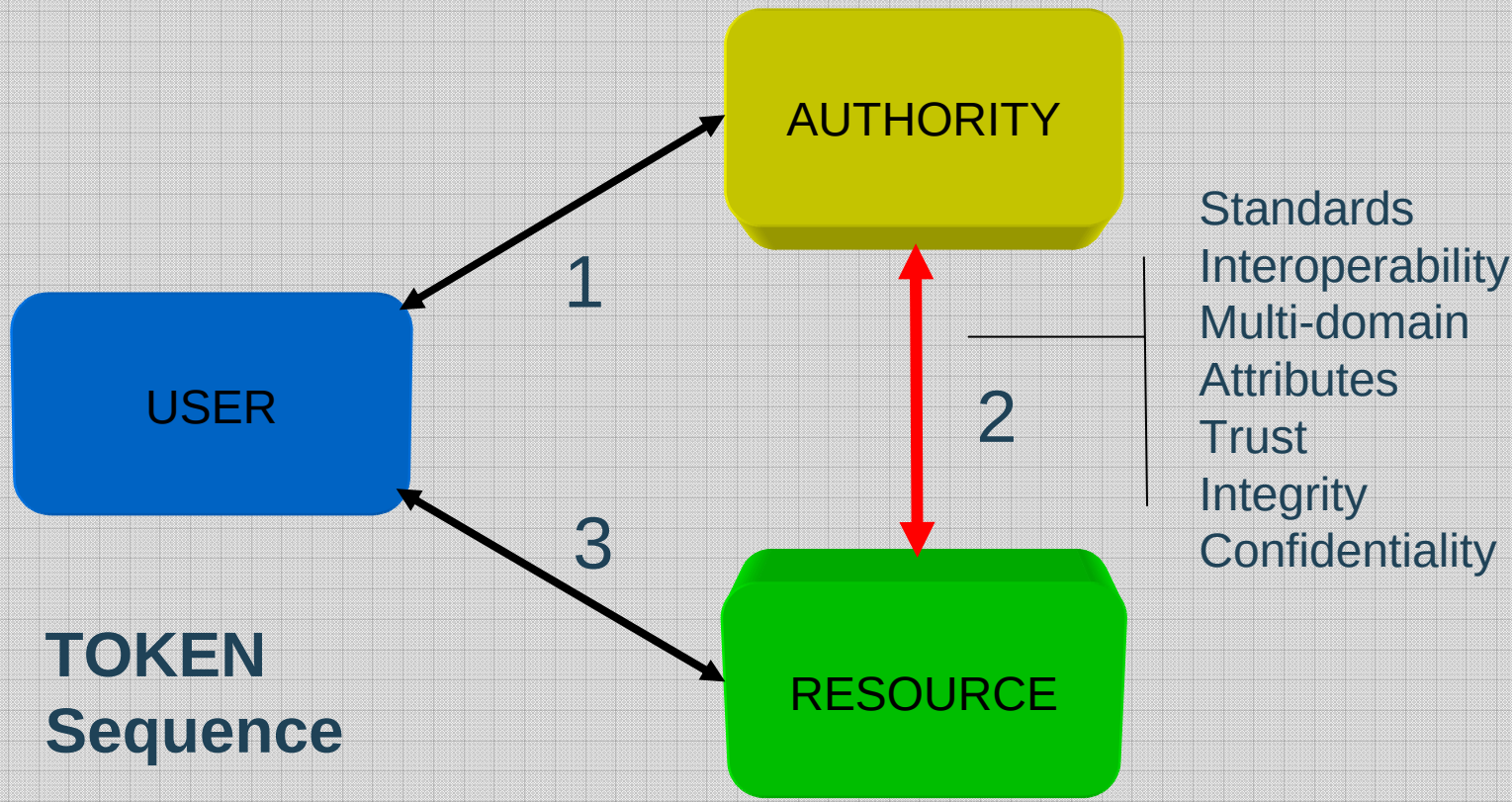
- Which sequences are applicable in WP 1,2 and 3 and describe them.
- Which (standard) message formats should be used where.
- What mechanisms are applicable where:
  - Inside the Authority, Resource and User
  - What (standards based) technology can be used to build required functions
  - Include multiple service domains that may work with different technologies
- How to further organize interactions with WP1, 2 and 3
  - Common organized inter-WP meetings ?
  - WP 4 specific meetings ?
- When / where / how frequent ?
- Intentions to setup collaborations with organizations outside project that are not EU funded such as Internet2, DRAGON - how to proceed ?

Next presentation #1: Mihai Cristea

- Router based Processing of IP Packets with tokens
- Router may use FORCES architecture



Next presentation #2: Yuri Demchenko



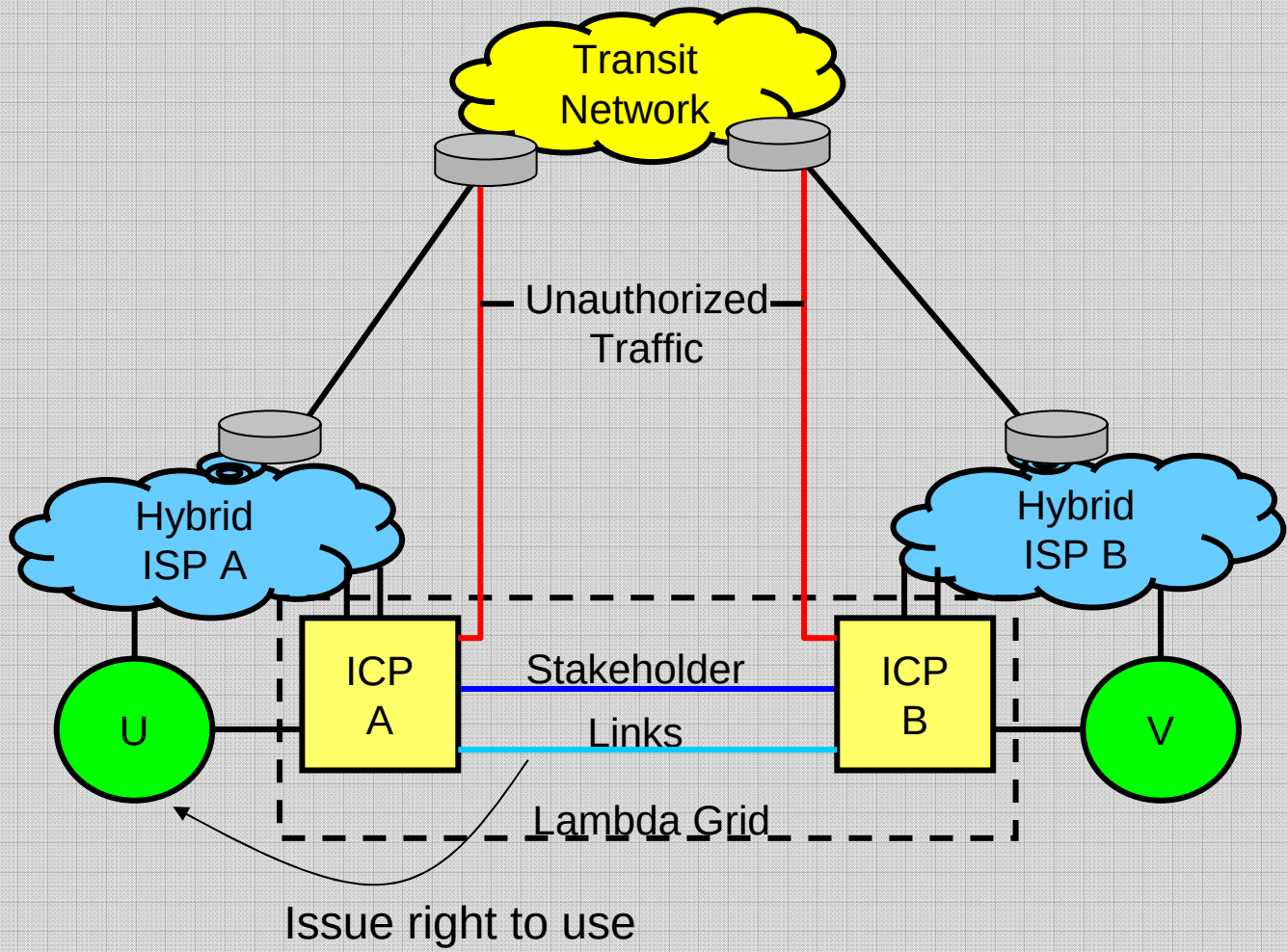
PHOSPHORUS

Efficiency and Performance Issues in Token Based Switch Systems

Mihai Cristea
University of Amsterdam

PHOSPHORUS Kick-off meeting - Poznan 17-18 October 2006

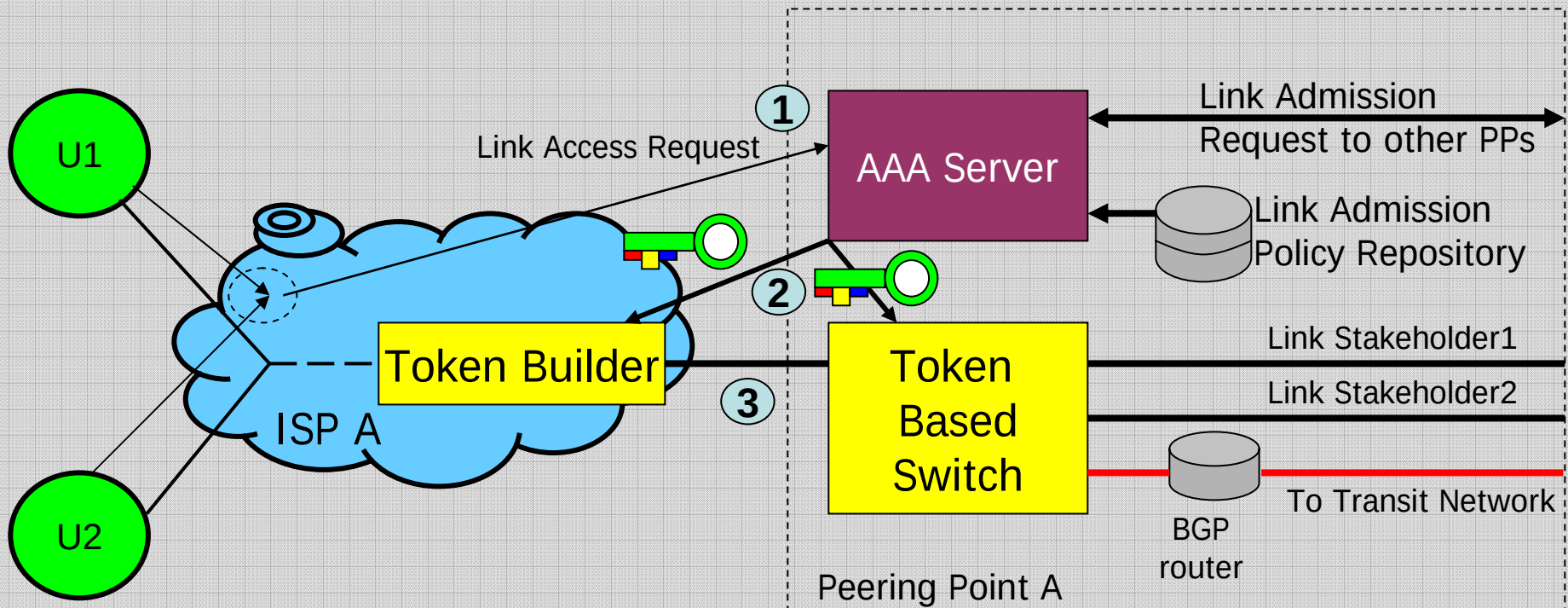
Token based path selection at interconnection points - demo at SC-05



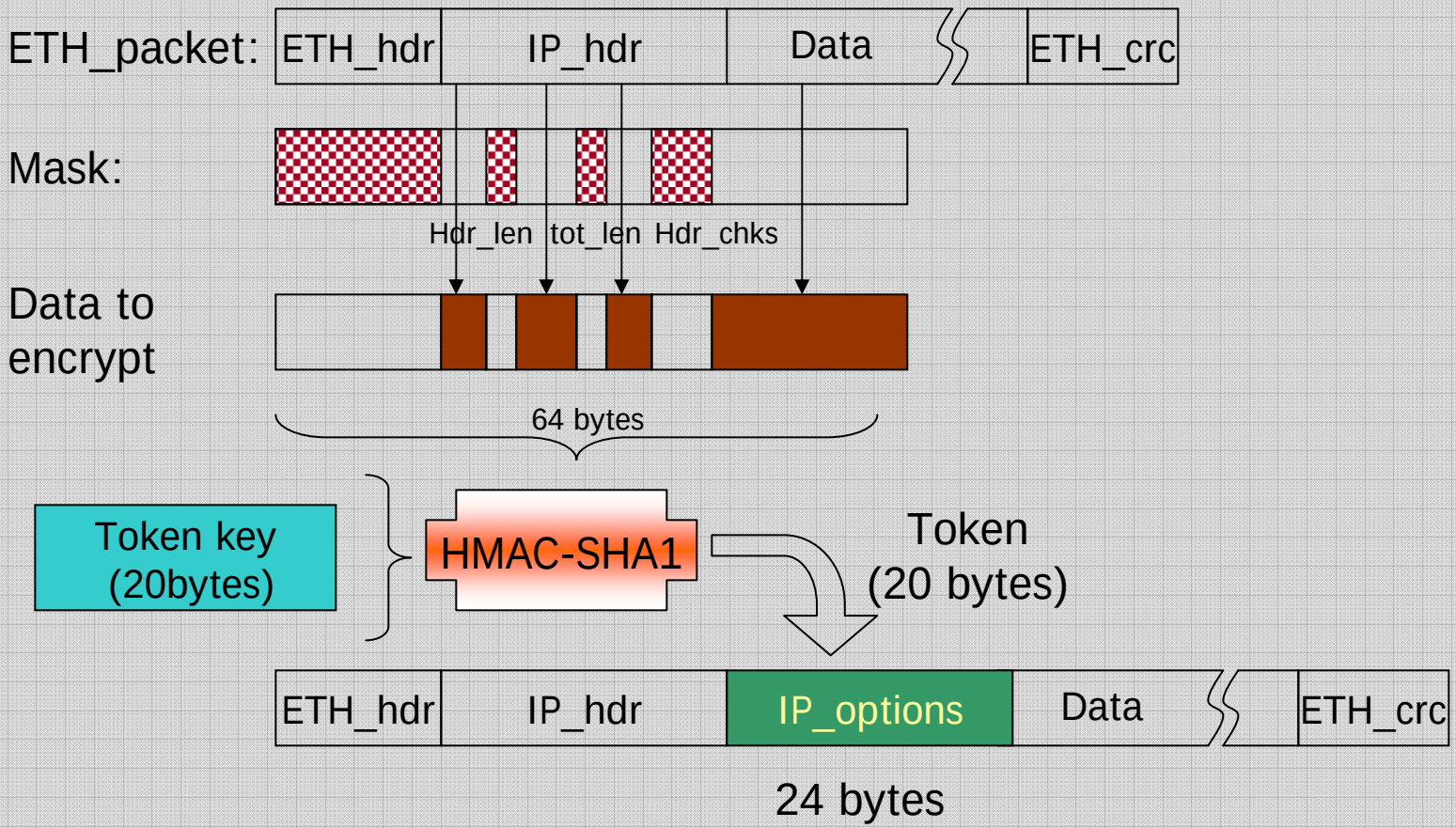
Why tokens?

- Tokens are a simple way to authorise resource usage;
- Can bind to differrent semantics;
- Decouple time of authorisation from time of use.

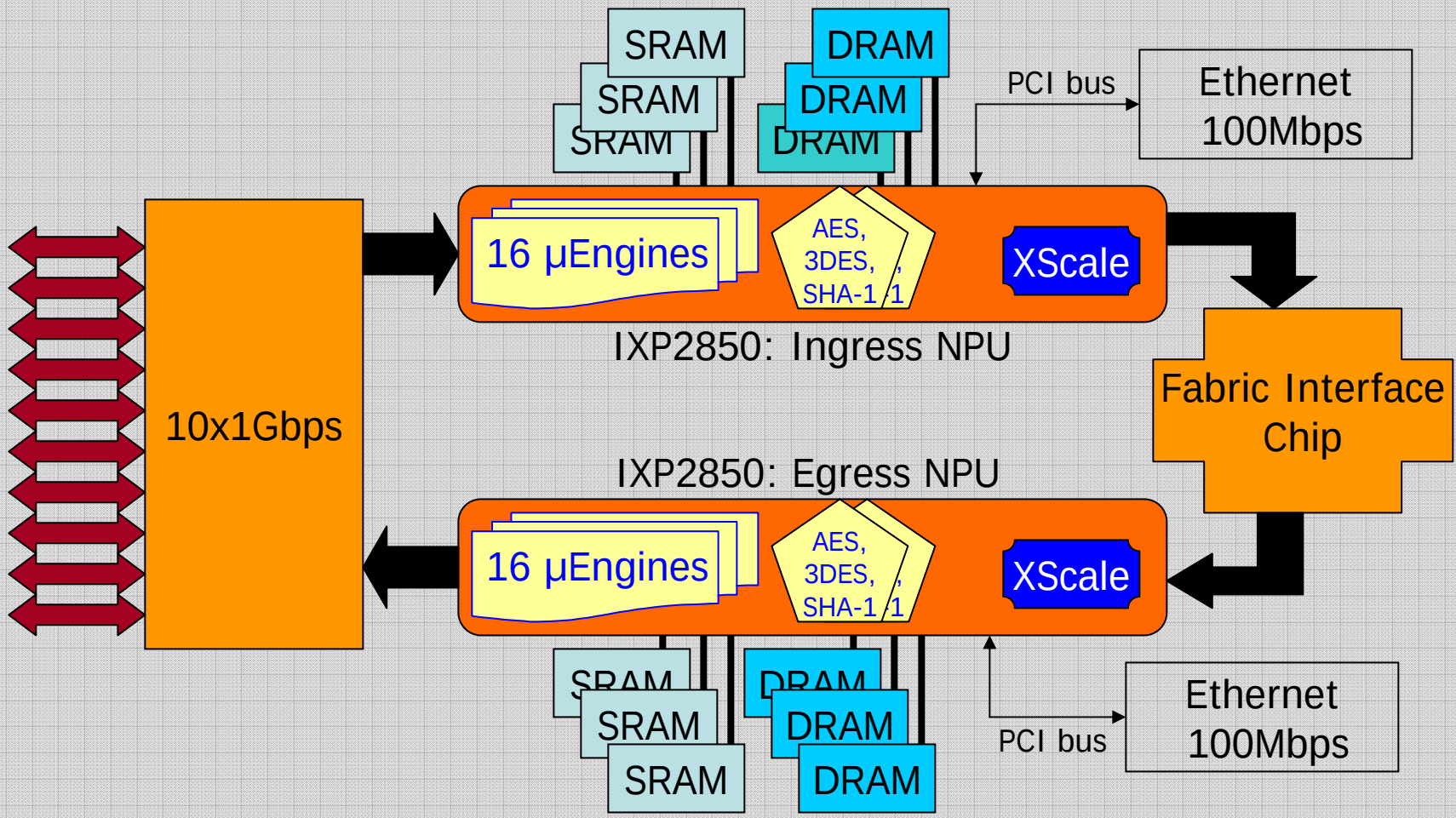
TBS Architecture



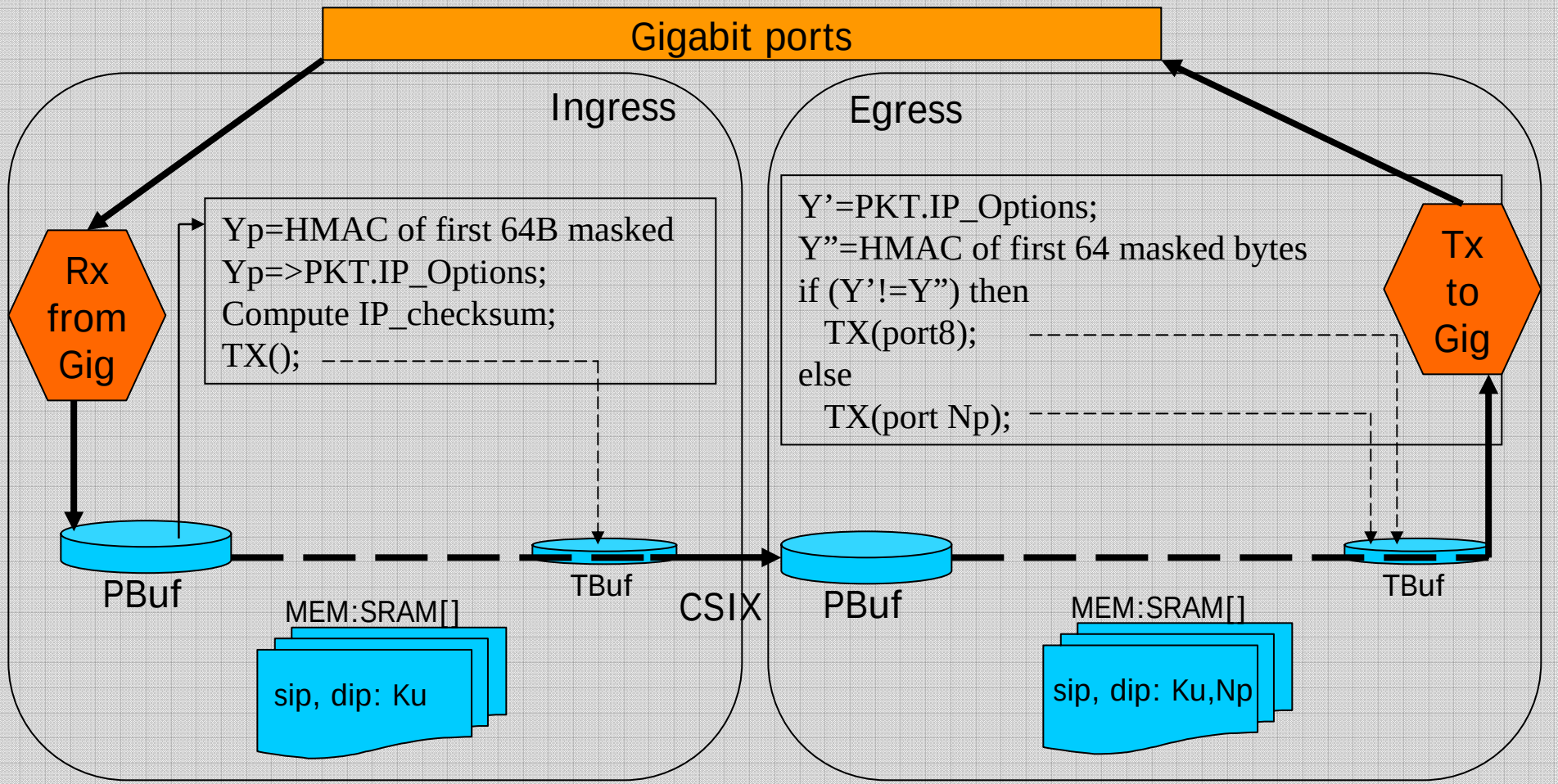
Token creation



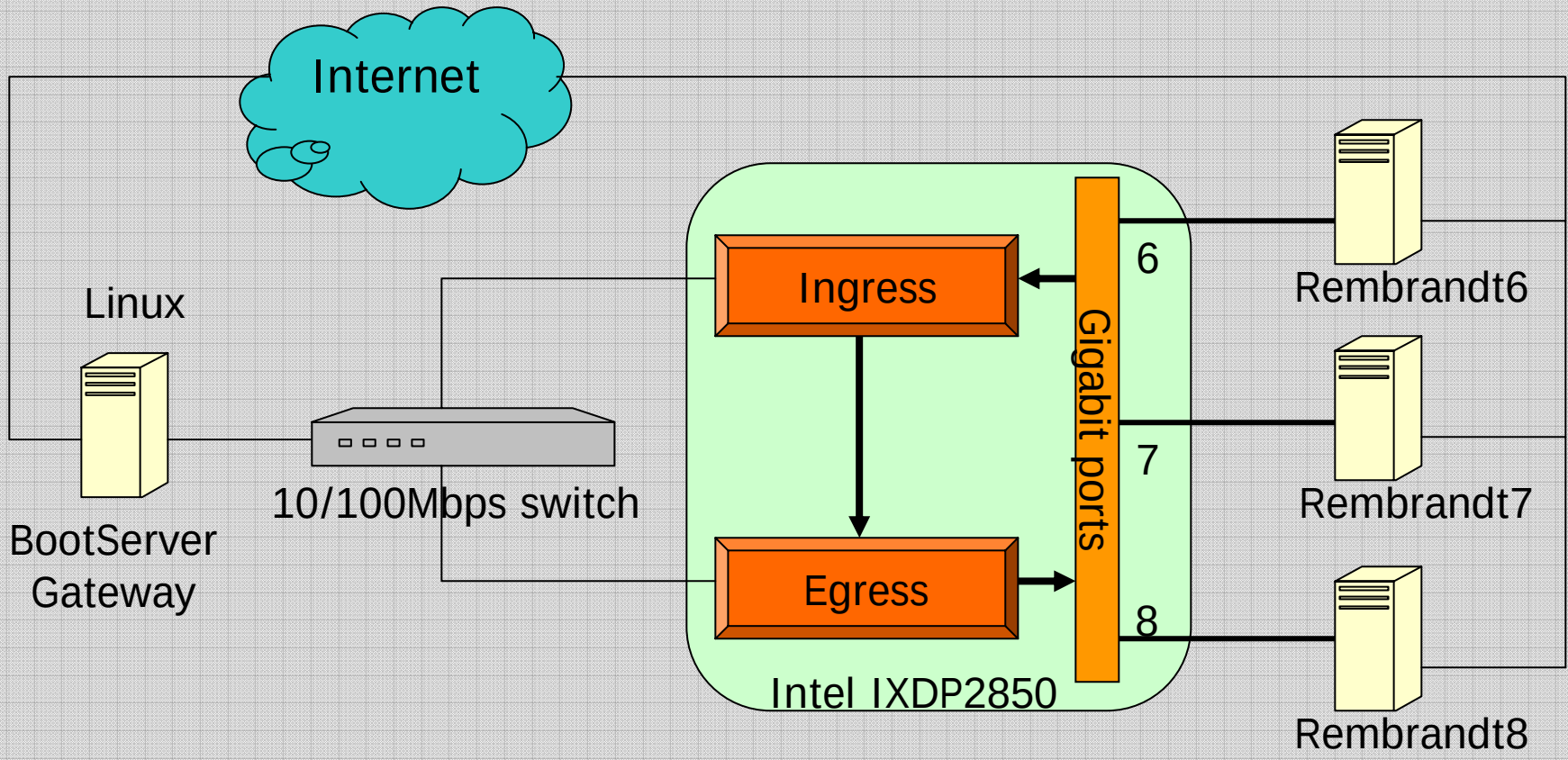
HW platform: IXDP2850



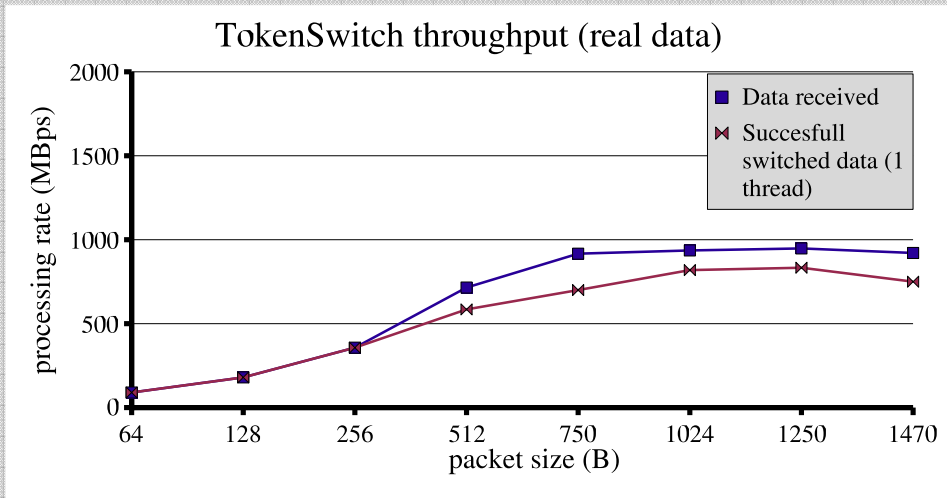
TokenSwitch application

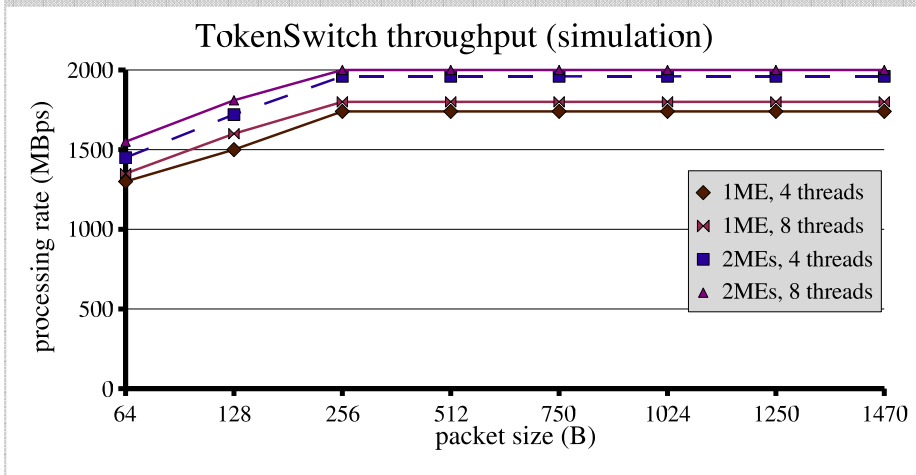


SuperComputing 2005 Demo



Performance





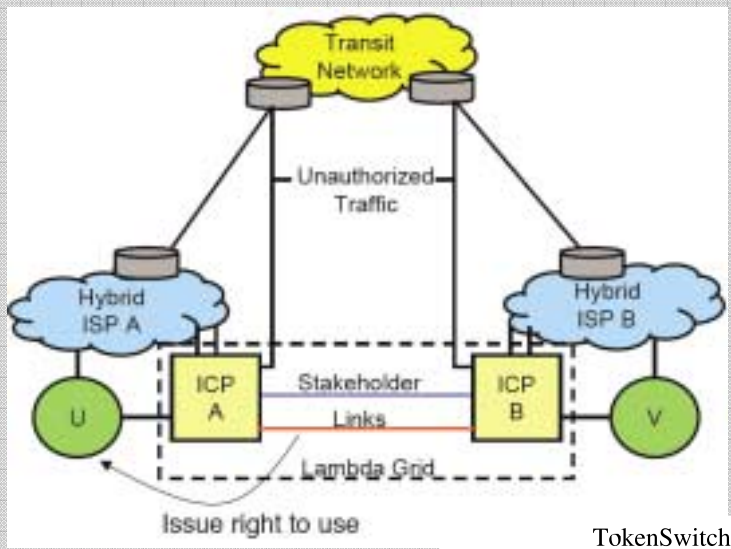
Work inside Phosphorus

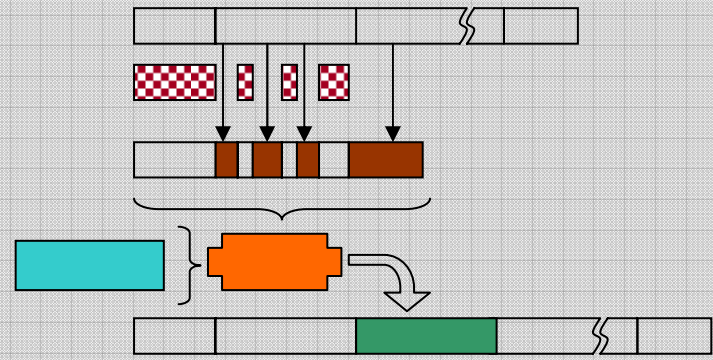
- Building a Token Based Router – an IP service using an IETF ForCES based forwarding device:
  - ForCES describes a framework (RFC 3746) for modular data forwarding devices.
  - Data forwarding functions implement routing, bridging, signaling, access control functions, etc.
  - Token recognition can be another functional block

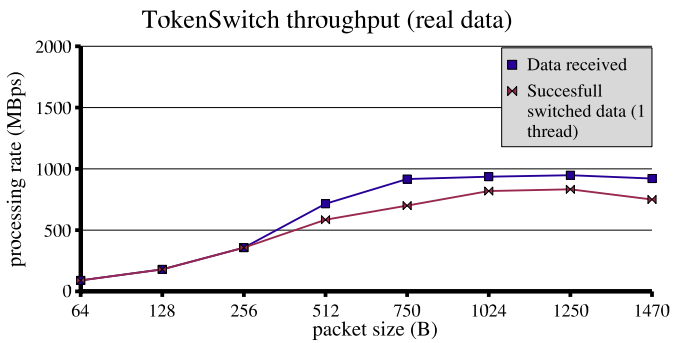
Conclusion

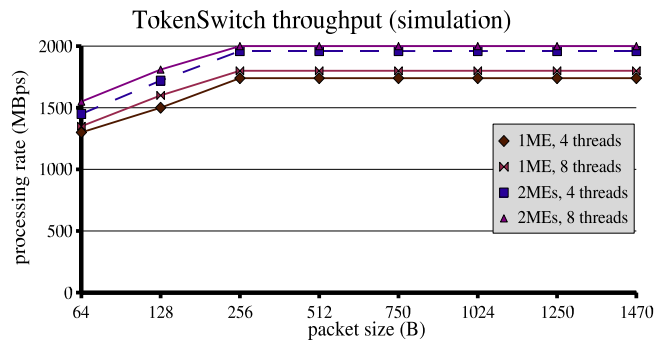
- Token Based Switching application on network processors:
  - Select an optical path in hybrid networks;
  - Admission control based on tokens;
  - Multi-Gigabit speeds;
  - Dynamically set up multiple shortcuts across a multi-domain end-to-end connection.

Questions ?


Transit Network
Unauthorized Traffic
Hybrid ISP A
Hybrid ISP B
ICP A
ICP B
Stakeholder
Links
Lambda Grid
U
V
Issue right to use

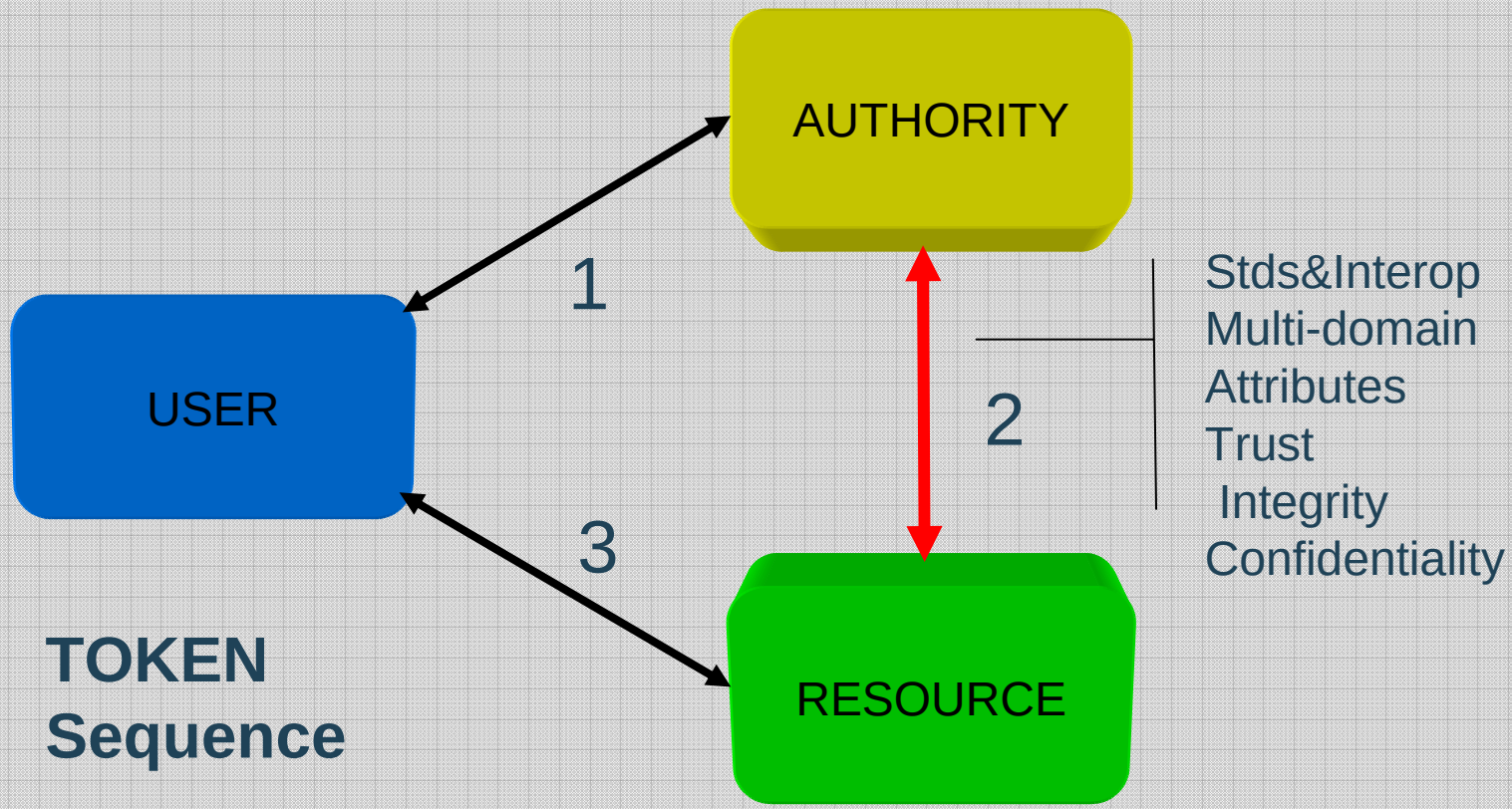



TokenSwitch throughput (real data)
processing rate (MBps)
packet size (B)
Data received
Succesfull switched data (1 thread)
2000
1500
1000
500
0
64
128
256
512
750
1024
1250
1470


TokenSwitch throughput (simulation)
processing rate (MBps)
packet size (B)
1ME, 4 threads
1ME, 8 threads
2MEs, 4 threads
2MEs, 8 threads
2000
1500
1000
500
0
64
128
256
512
750
1024
1250
1470

Next presentation #2: Yuri Demchenko

- GAAA-AuthZ components to support Complex Resource Provisioning (CRP)
- Assertions format between Authority and Resource Policy Enforcement Point



PHOSPHORUS

GAAA-AuthZ components to support Complex Resource Provisioning (CRP)

Yuri Demchenko <demch@science.uva.nl>
System and Network Engineering Group
University of Amsterdam

POSPHORUS kick-off meeting, 17-18 October 2006, Poznan

Outline

- Background information - Affiliated and previous projects
  - Moving to multi-domain dynamic AAA service infrastructure
- GAAA-AuthZ components to support dynamic security context mngnt
  - Extended AuthZ ticket format
  - AuthZ security context management in multidomain AuthZ
- Using TCG Trusted Computing and Trusted Network Connect platforms (TNC) for extending trusted application domain
- Using XACML policy format for multidomain access control
- Summary and Issues to discuss

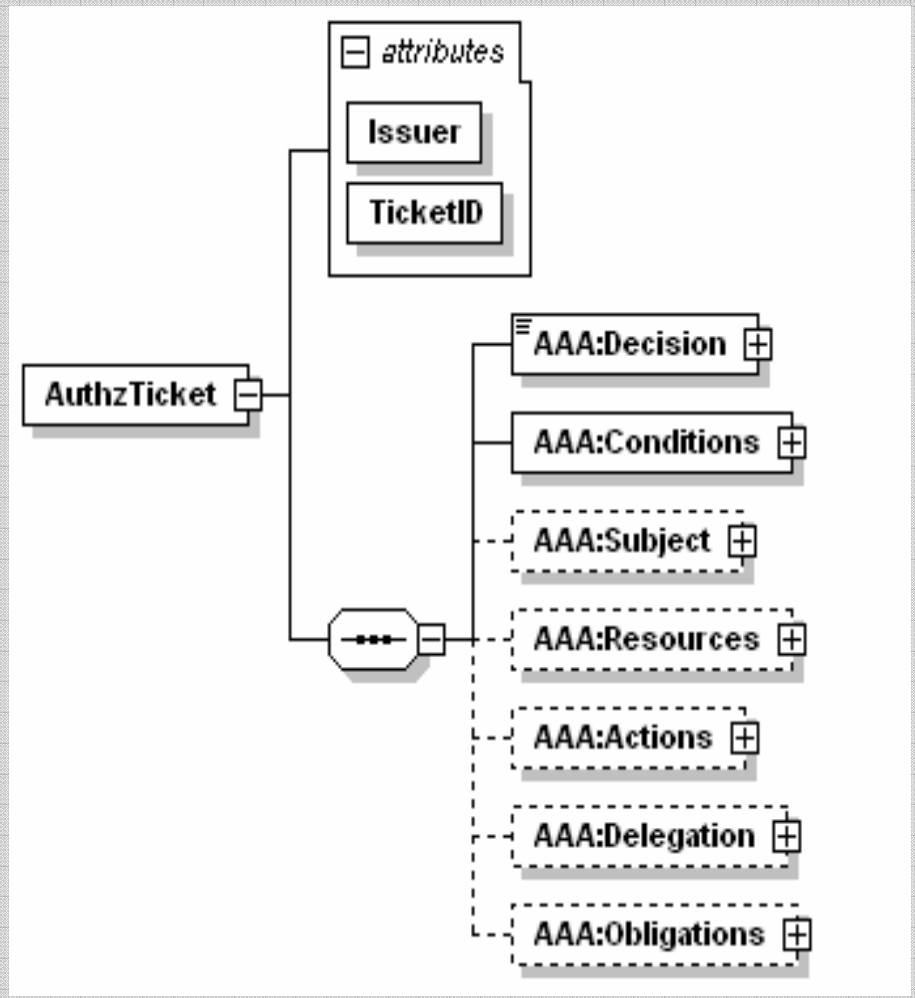
GAAA – Generic Authentication, Authorization, Accounting

GAAA-AuthZ – GAAA AuthZ Framework

Background information – Affiliated and previous projects

- EGEE-I and EGEE-II
  - EGEE gLite Java Authorisation Framework (gJAF)
    - gJAF extension to support SAML attributes, AuthZ session and full XACML policy functionality
    - Integration with the GT4-AuthZ framework
  - LCG/EGEE Operational Security and EGEE Grid Security Infrastructure
- OGSA-AuthZ WG contribution
  - Dynamic AuthZ service infrastructure and components
- GigaPort NG Research on Network
  - Gap analysis of Authorisation services functionality for Optical LightPath Provisioning (OLPP)
- Collaboratory.nl project - industry funded project
  - Multidomain resource administration for Collaborative applications

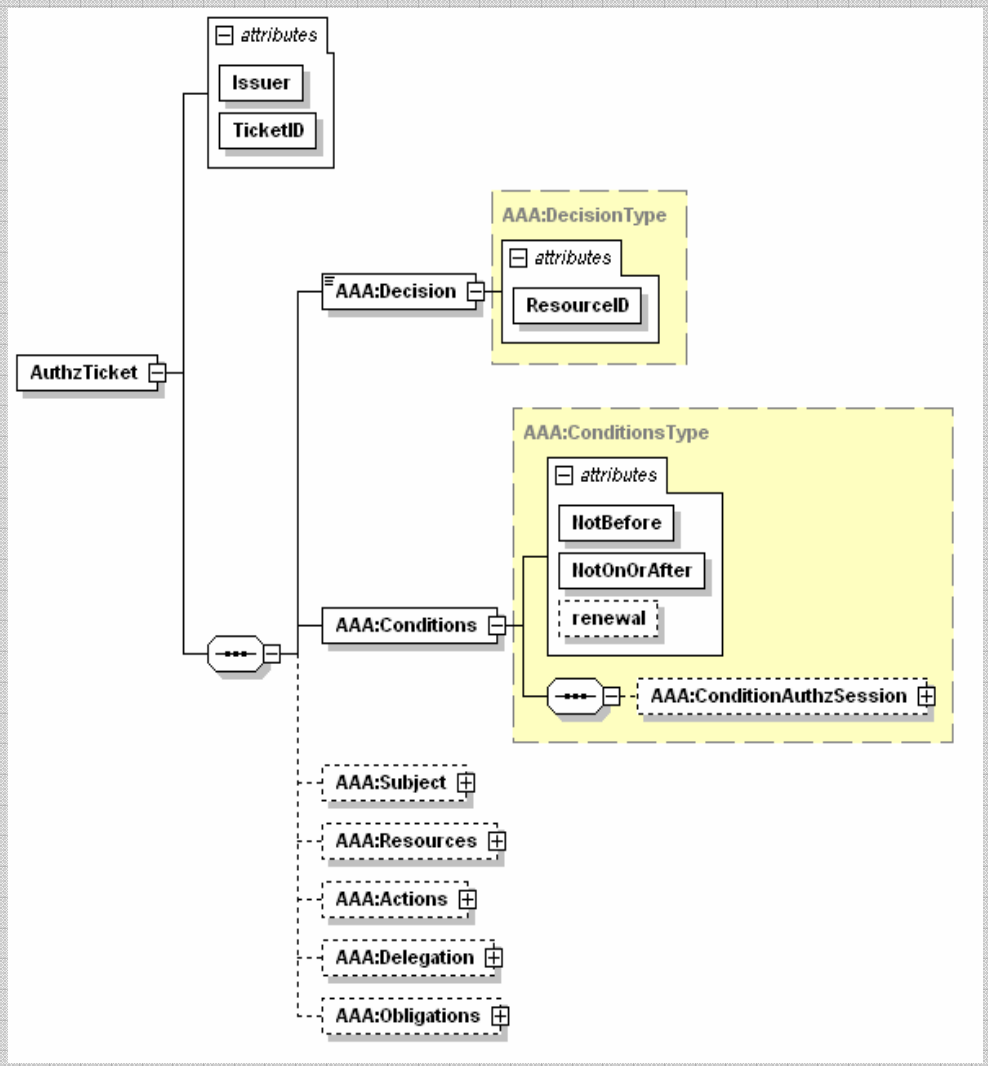
AuthZ ticket/assertion for extended security context management – Data model (1) - Top elements



Required functionality to support multidomain provisioning scenarios

- Allows multiple Attributes format (semantics, namespaces)
- Establish and maintain Trust relations between domains
  - Including Delegation
- Ensure Integrity of the AuthZ decision
  - Keeps AuthN/AuthZ context
  - Allow Obligated Decisions (e.g. XACML)
- Confidentiality
  - Creates a basis for user-controlled Secure session

AuthZ ticket Data model (2) - Mandatory elements



- TicketID attribute
- Decision element and Resource attribute
- Conditions Element and validity attributes
- Extensible element ConditionAuthzSession
  - Any AuthZ session related data

AuthZ ticket main elements

<Decision> element - holds the PDP AuthZ decision bound to the requested resource or service expressed as the ResourceID attribute.

<Conditions> element - specifies the validity constrains for the ticket, including validity time and AuthZ session identification and additionally context

- <ConditionAuthzSession> (extendable) - holds AuthZ session context

<Subject> complex element - contains all information related to the authenticated Subject who obtained permission to do the actions

- <Role> - holds subject's capbilities
- <SubjectConfirmationData> - typically holds AuthN context
- <SubjectContext> (extendable) - provides additional security or session related information, e.g. Subject's VO, project, or federation.

<Resources>/<Resource> - contains resources list access to which is granted by the ticket

<Actions>/<Action> complex element - contains actions which are permitted for the Subject or its delegates

<Delegation> element – defines who the permission and/or capability are delegated to: another Subjects or community

- attributes define restriction on type and depth of delegation

<Obligations>/<Obligation> element - holds obligations that PEP/Resource should perform in conjunction with the current PDP decision.

Security context management in multidomain AuthZ: Context dependent information and existing mechanisms

- Context dependent information/attributes:
  - Policy
  - Trust domains and authorities
  - Attributes namespaces
  - Service/Resource environment/domain
  - Credential semantics and formats

- Mechanisms to transfer/manage context related information
  - Service and requestor/user ID/DN format that should allow for both using namespaces and context aware names semantics
  - Attribute format (either X.509/X.521 or URN/SAML2.0 presentation)
  - Context aware XACML policy definition using the Environment element of the policy Target element
  - Security tickets and tokens used for AuthZ session management and for provisioned resource/service identification
  - Security federations for users and resources, e.g. VO membership credentials

Extending trusted application domain with TCG and TNC

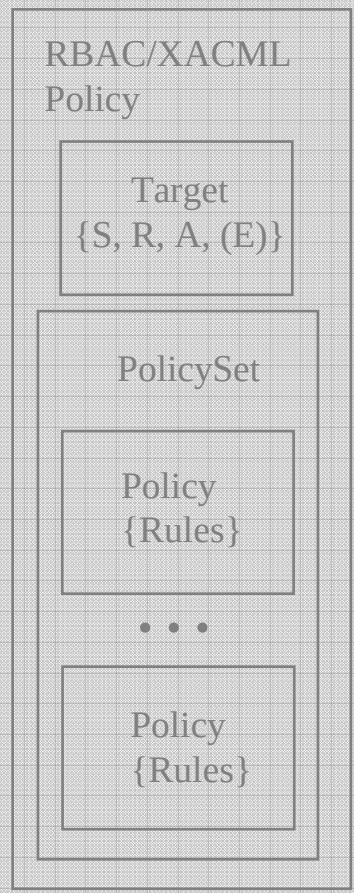
- TCG Trusted Computing platform (TCG) and Trusted Network Connect platform (TNC) can create a basis for trusted user/authority and resource/provider platforms introduction
  - TPM ensured remote platform integrity will allow to initiate trusted provisioning/AuthZ session for AAA services
  - Includes three stages
    - (1) Remote platform inspection/verification (TCG and TNC)
    - (2) Starting User session and Virtual WorkSpace Service (VWSS)
      - Provides secure executive environment for the user applications
    - (3) Starting Application session (GAAA-AuthZ)
      - Ensure Integrity and Confidentiality for the user application data

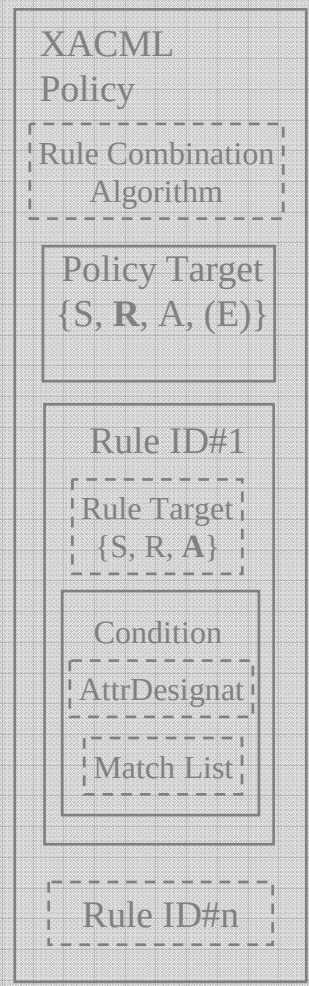
XACML Special profiles for RBAC and complex Resources

- XACML RBAC profile
  - defines policies that require multiple Subjects and roles combination to access a resource and perform an action
  - implements hierarchical RBAC model when some actions require superior subject/role approval to perform a specific action
  - can significantly simplify rights delegation inside the group of collaborating entities/subjects
- XACML Hierarchical Resource profile
  - defines policy format for hierarchically organised resources, e.g. file system or XML-based repositories
- XACML complex Resource profile
  - allows for complex request to multiple resources having the same request context, however decision is provided per resource
- XACML3 Policy Administration and Delegation profile

XACML Policy structure

- XACML Policy format





Summary and Issues to discuss

- GAAA-AuthZ/GAAA-P model and basic GAAA_tk components are available to support Complex Resource Provisioning and dynamic AuthZ services invocation
  - Need some work to integrate with the GMPLS control plane
  - Provisioning scenario and provisioning/AuthZ session defintion
  - Extending AuthZ ticket format for basic GMPLS scenarios
- Policy format for multidomain GMPLS provisioning use cases
  - XACML policy profile – is XACML usable here?
- TCG Trusted Computing platform (TCG) and Trusted Network Connect platform (TNC)
  - Can we benefit from these technologies?