Generic AAA Architecture
draft-delaat-aaa-generic-00

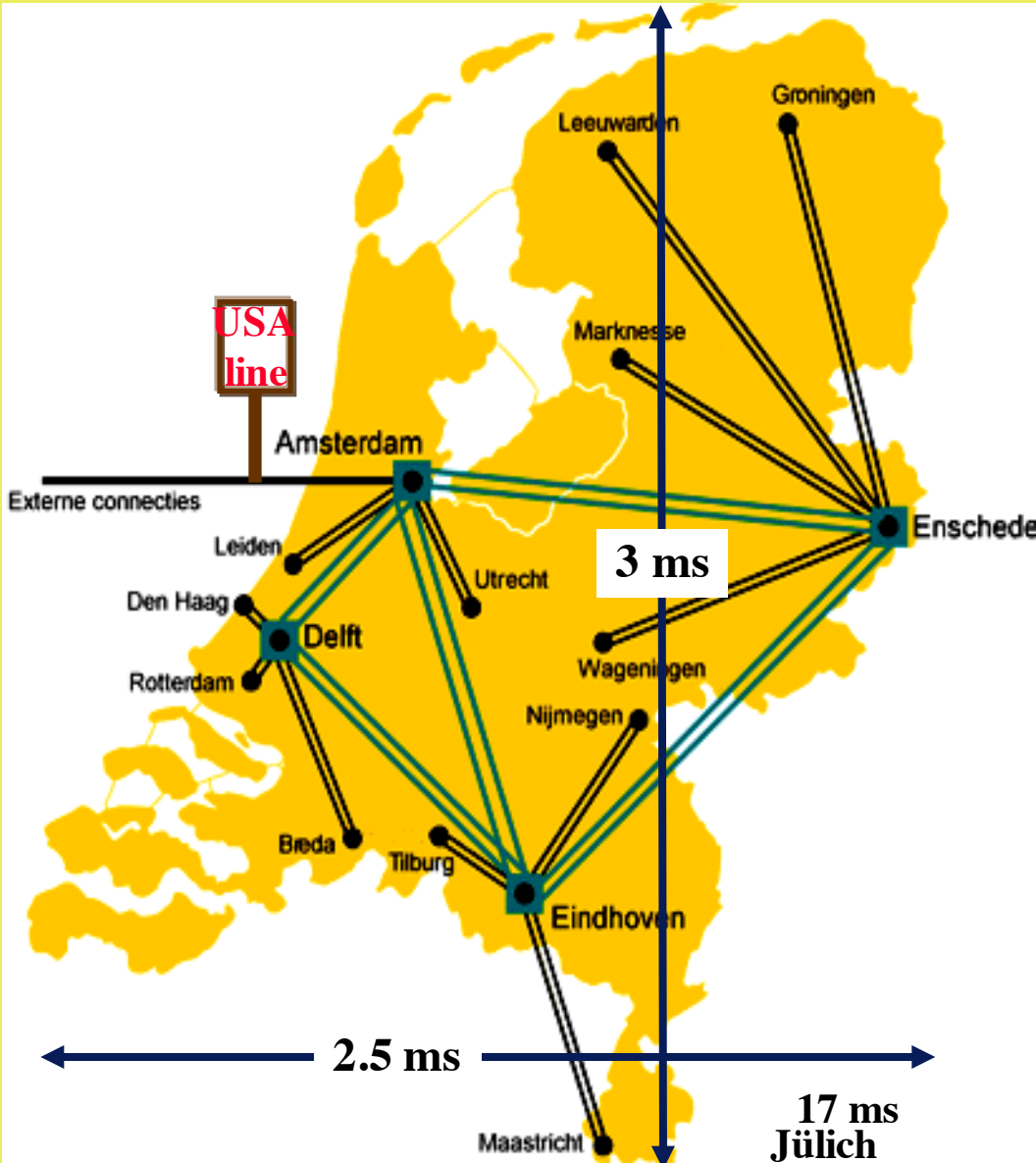
C. de Laat
Utrecht University
G. Gross
Lucent Technologies
L. Gommans
Cabletron Systems EMEA
J. Vollbrecht
Merit Network, Inc.
D. Spence
Merit Network, Inc.

Starting point

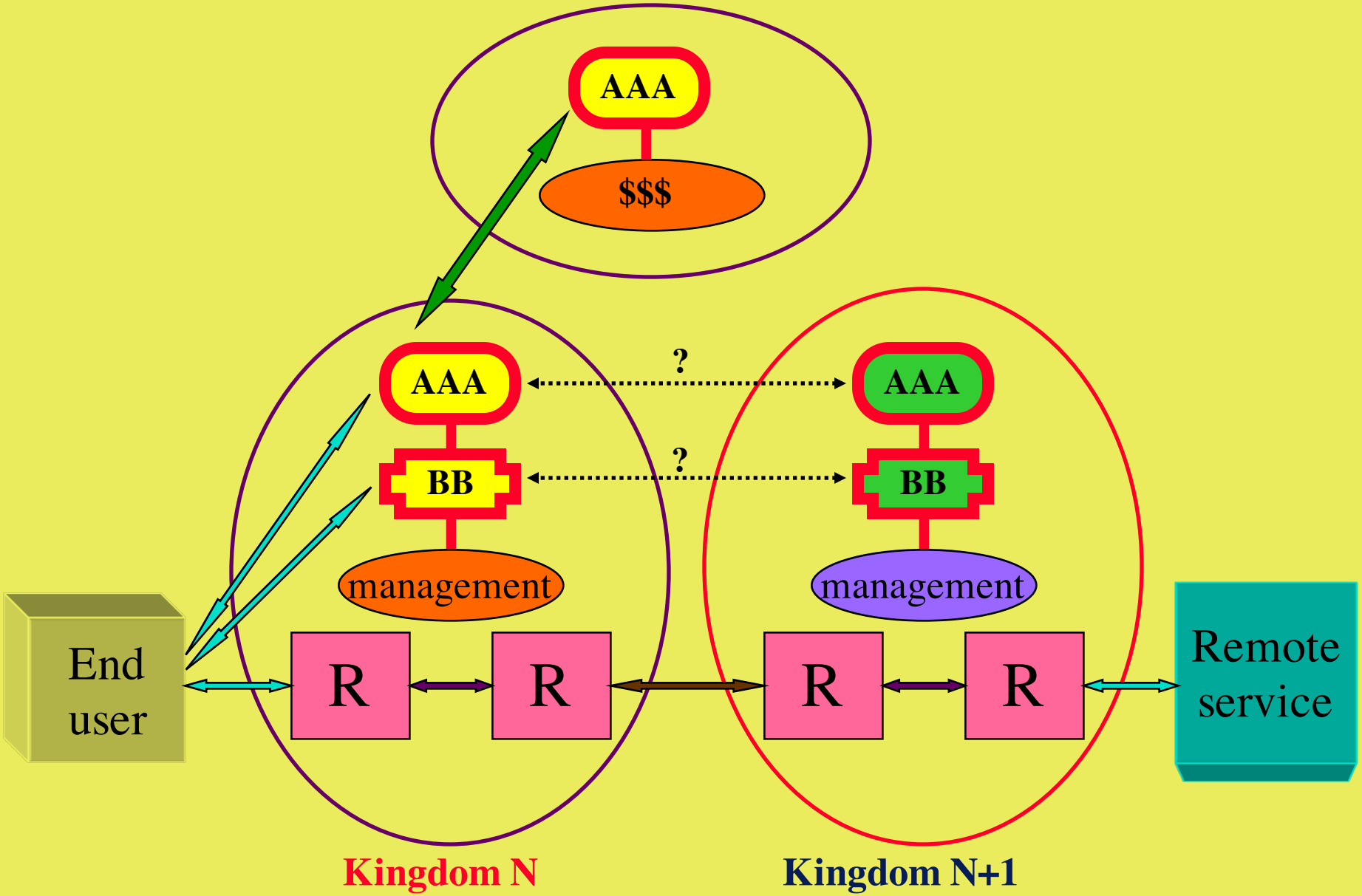
- **Applications**
  - Network Access
  - Bandwidth Broker
  - Authorization of resources living in many administrative domains
  - Budget system
  - Library system
  - Computer based education system
- **Requirements**
  - Take high level requirements from the different applications as notified in the AAA drafts
  - Separate common from application specific functionality

Physics-UU to IPP-FZJ => 7 kingdoms

- Physics dept
- Campus network
- SURFnet
- TEN 155
- WINS/DFN
- Juelich, Campus
- Plasma Physics

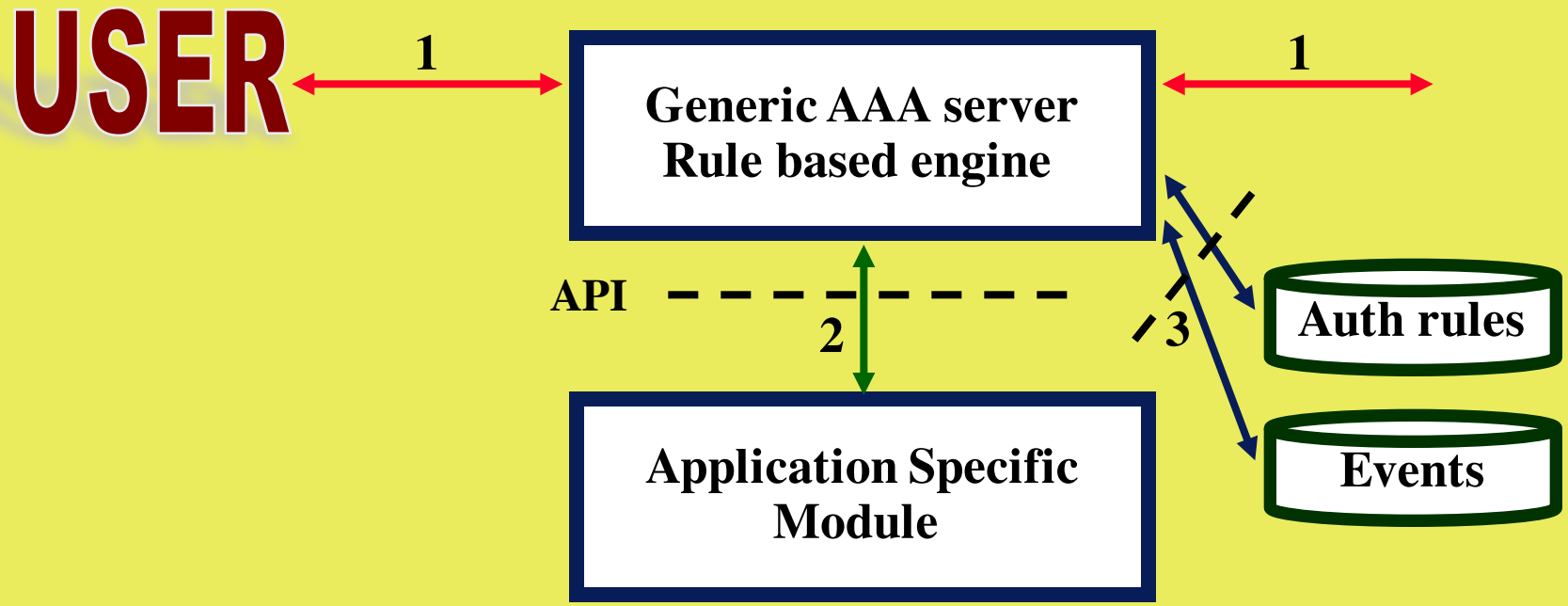


The need for AAA



AAA Server building block

Rule example: Auth_A = (B>9) .or. C .and. D



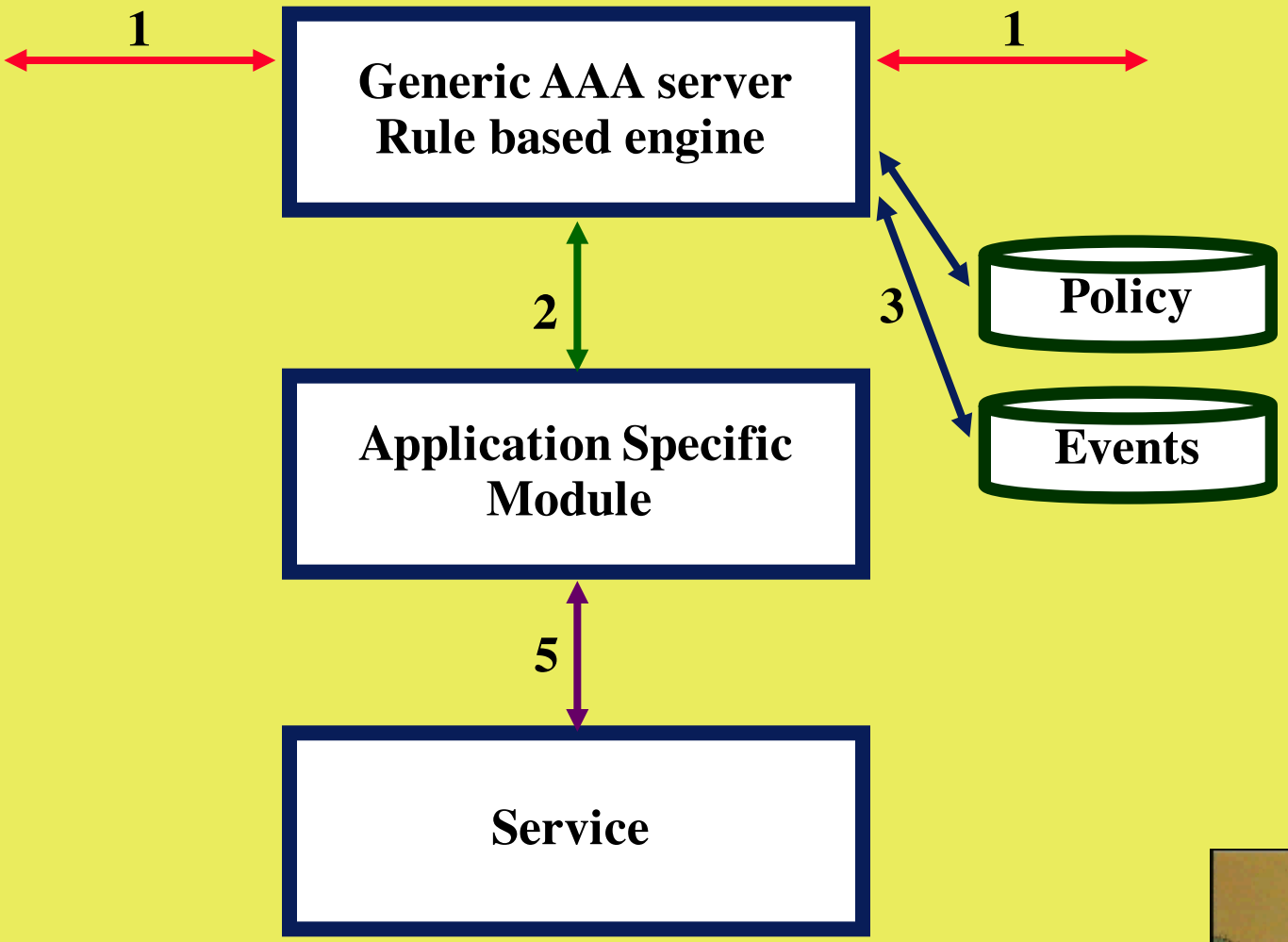
Types of communication:

1: "The" AAA protocol

2: interface (API) to app specific module (addressing!)

3: interface (API or connection) to repositories (e.g. LDAP)

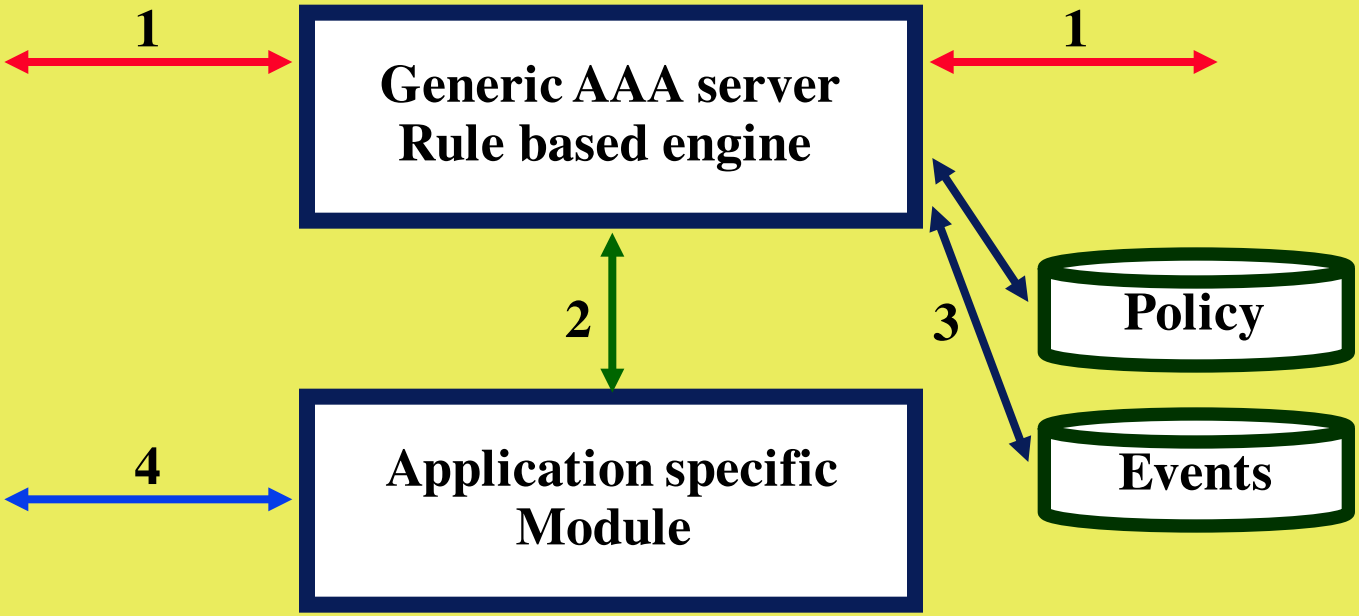
Pushing the buttons



Types of communication:

5: Towards service (f.e. COPS, CLI, SNMPv3)

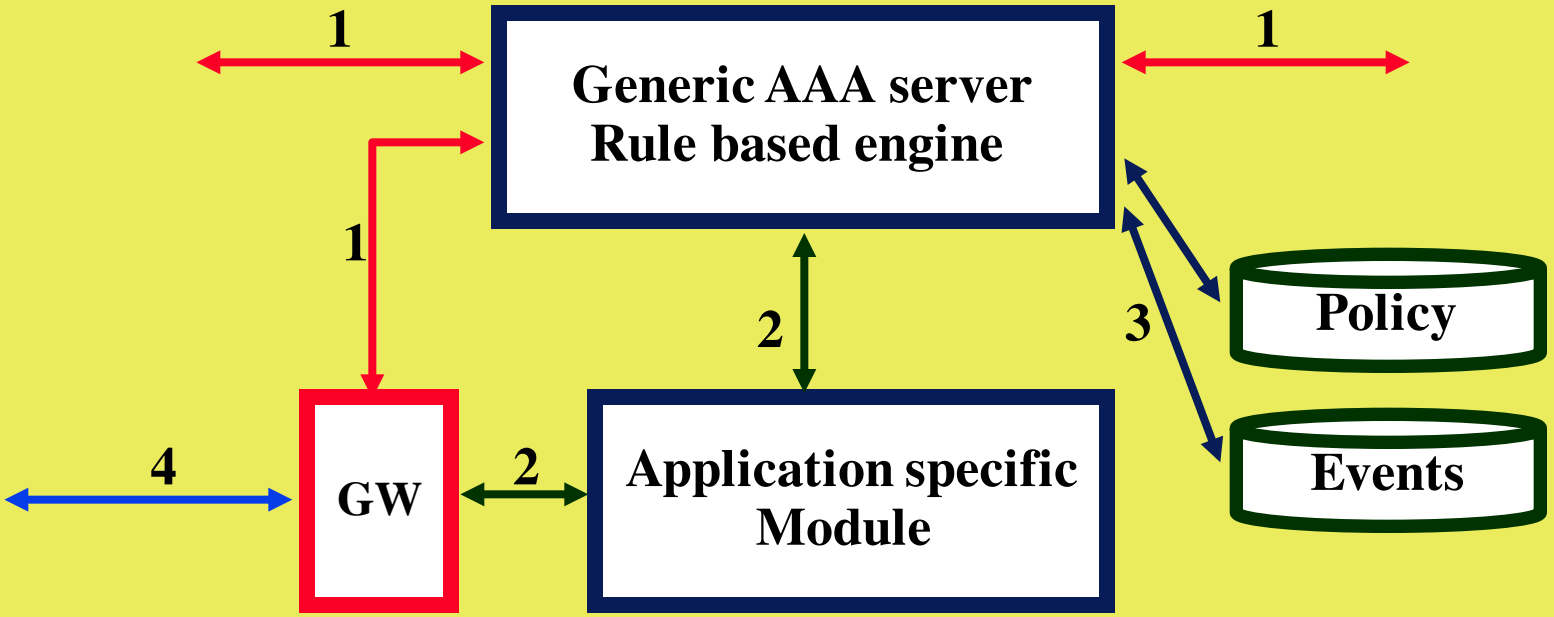
Legacy protocols



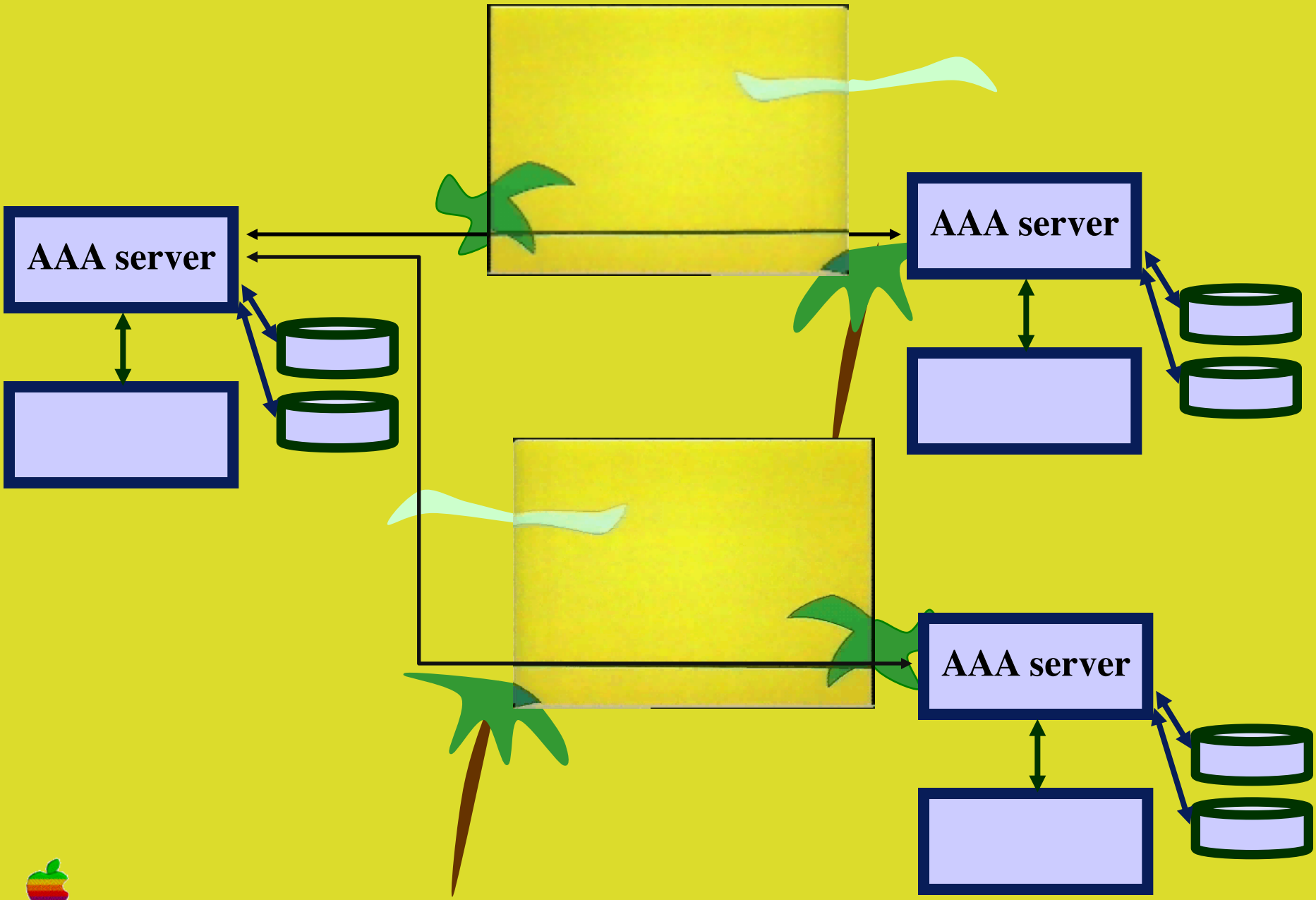
Types of communication:

4: Legacy protocols (Radius, Diameter, …)

Gateway


1
Generic AAA server
Rule based engine
1
1
2
3
Policy
Events
4
GW
2
Application specific
Module

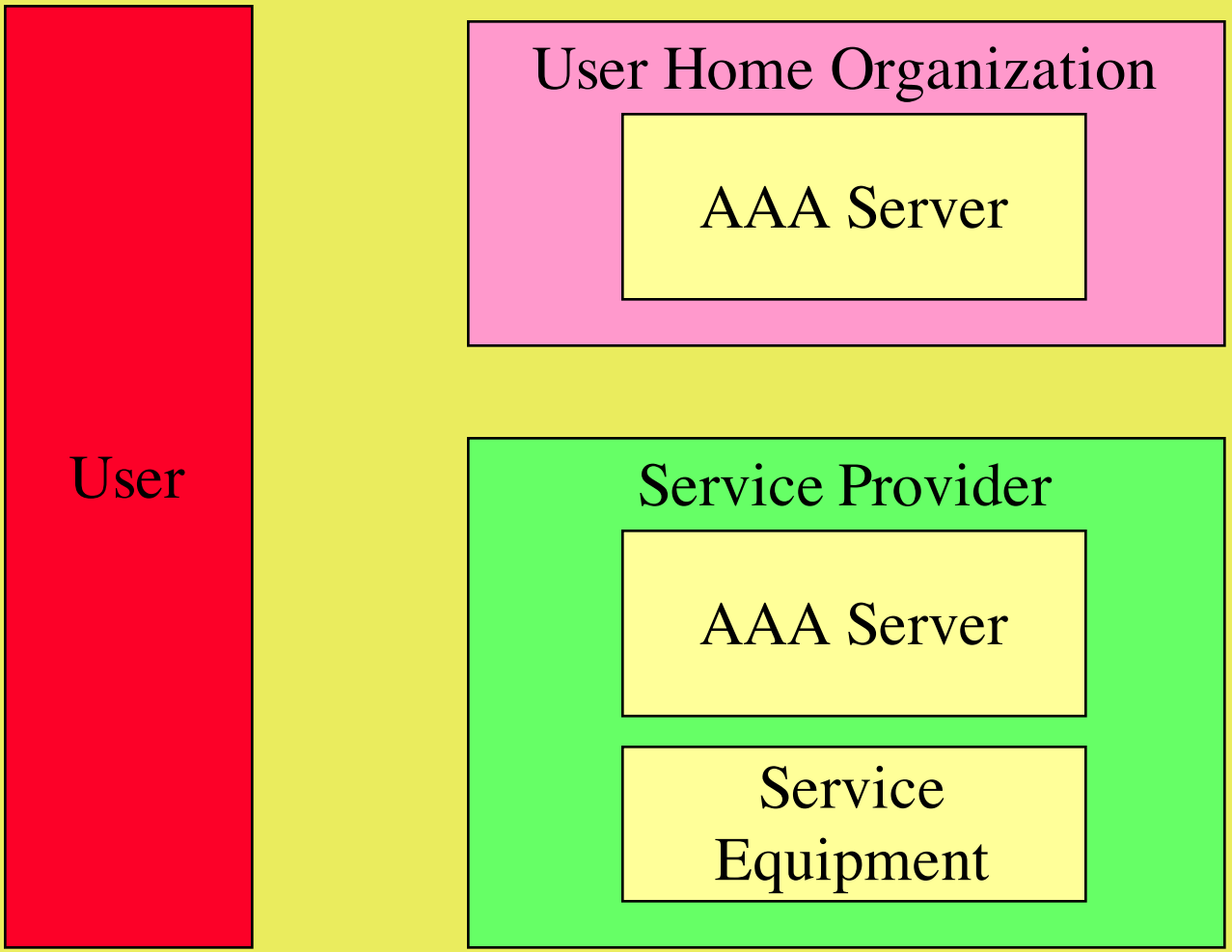
Generic AAA Agent Model



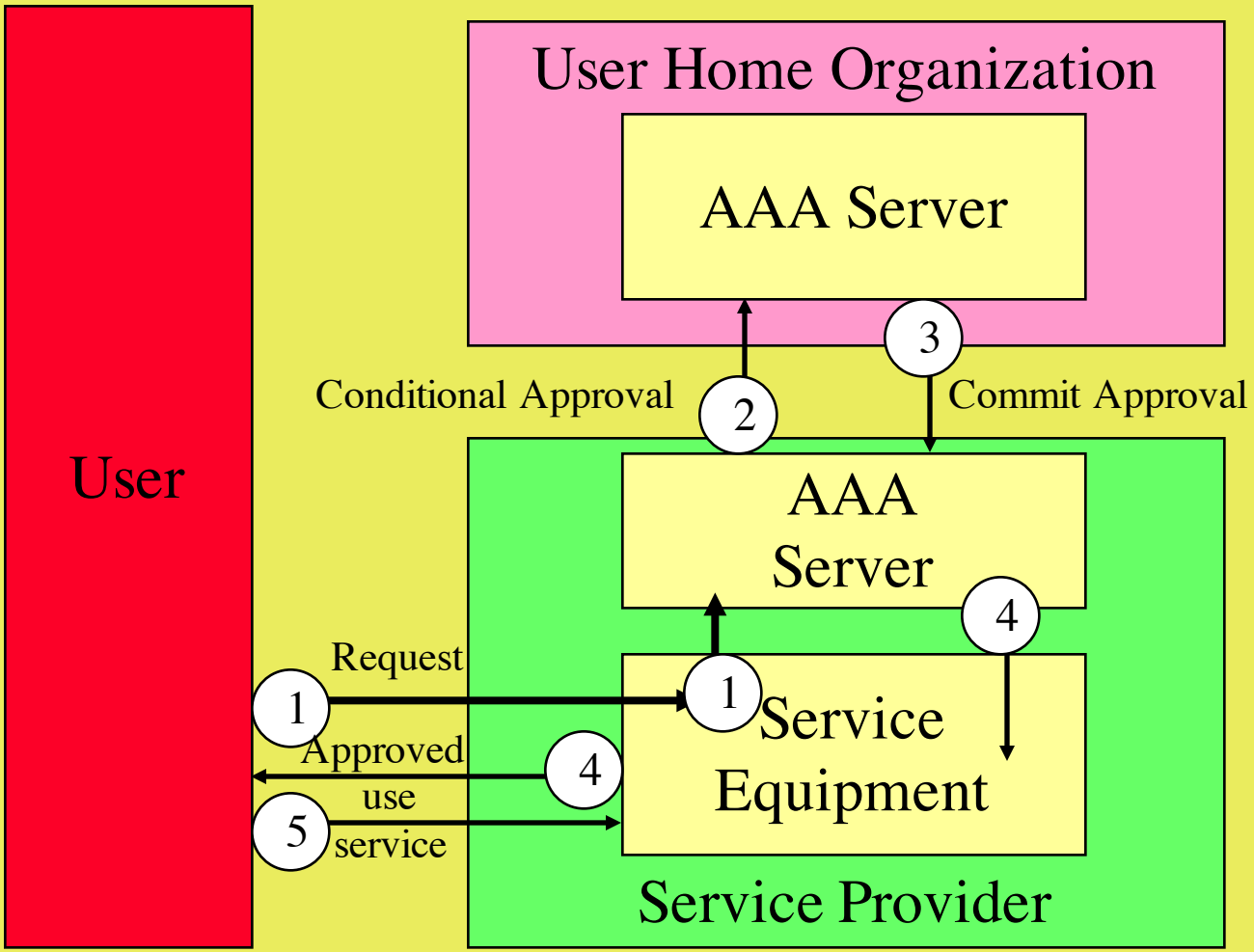
- We will now examine the generic AAA problem from the perspective of a layered protocol model

George Gross

Basic Authorization Entities

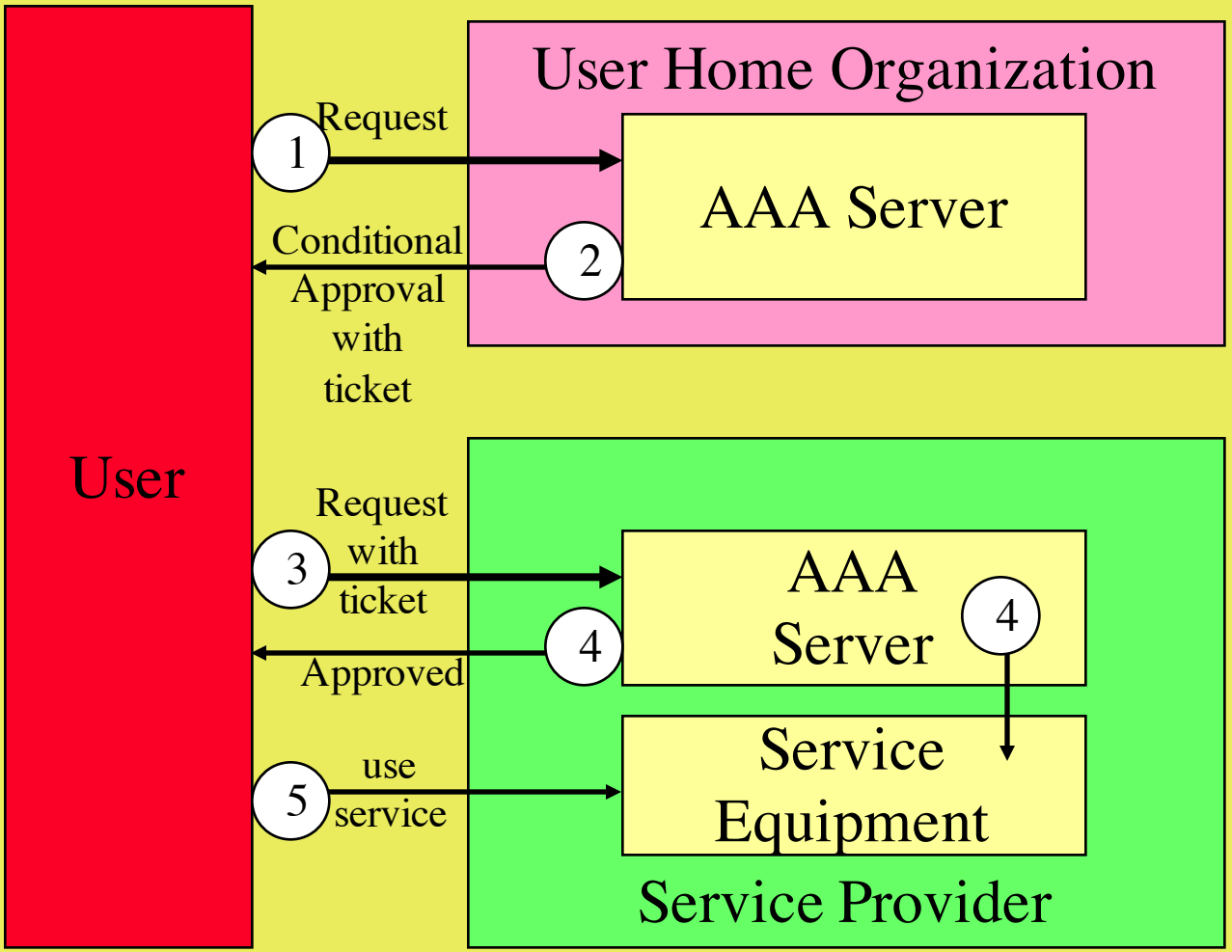


Roaming "Pull" Authorization Model



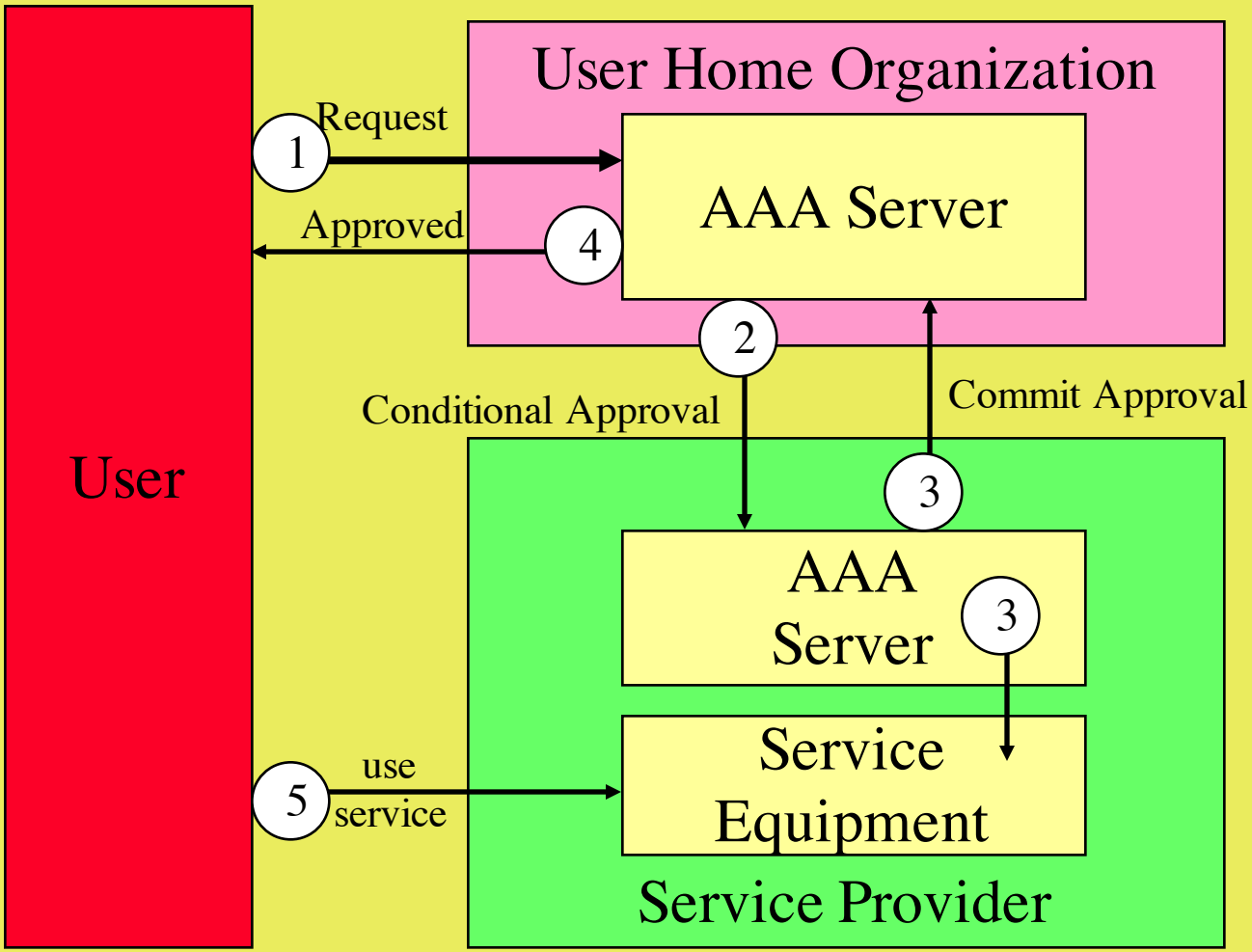
Example applications: Mobile IP, PPP dial-in to NAS

Roaming "Push" Authorization Model



Example application: Internet printing, where file and print servers are in different admin domains

Roaming "Agent" Authorization Model



Example application: bandwidth brokerage at Enterprise/Service Provider boundary

Complex Authorization Message Flows

- The authorization models just discussed dealt with a single type of application request that had only two stakeholders
- But an authorization request could contain multiple application requests of different types, and arbitrary chains of stakeholders.
- Example, grant the authorization request if the following logical expression evaluates to true:
  - User's request for QoS bandwidth is available given network's state
  - AND (User's account "A" has credit to pay for it OR account "B" has credit to pay for it)
  - AND User Home Organization has less than its contracted bandwidth ceiling allocated by the Service Provider

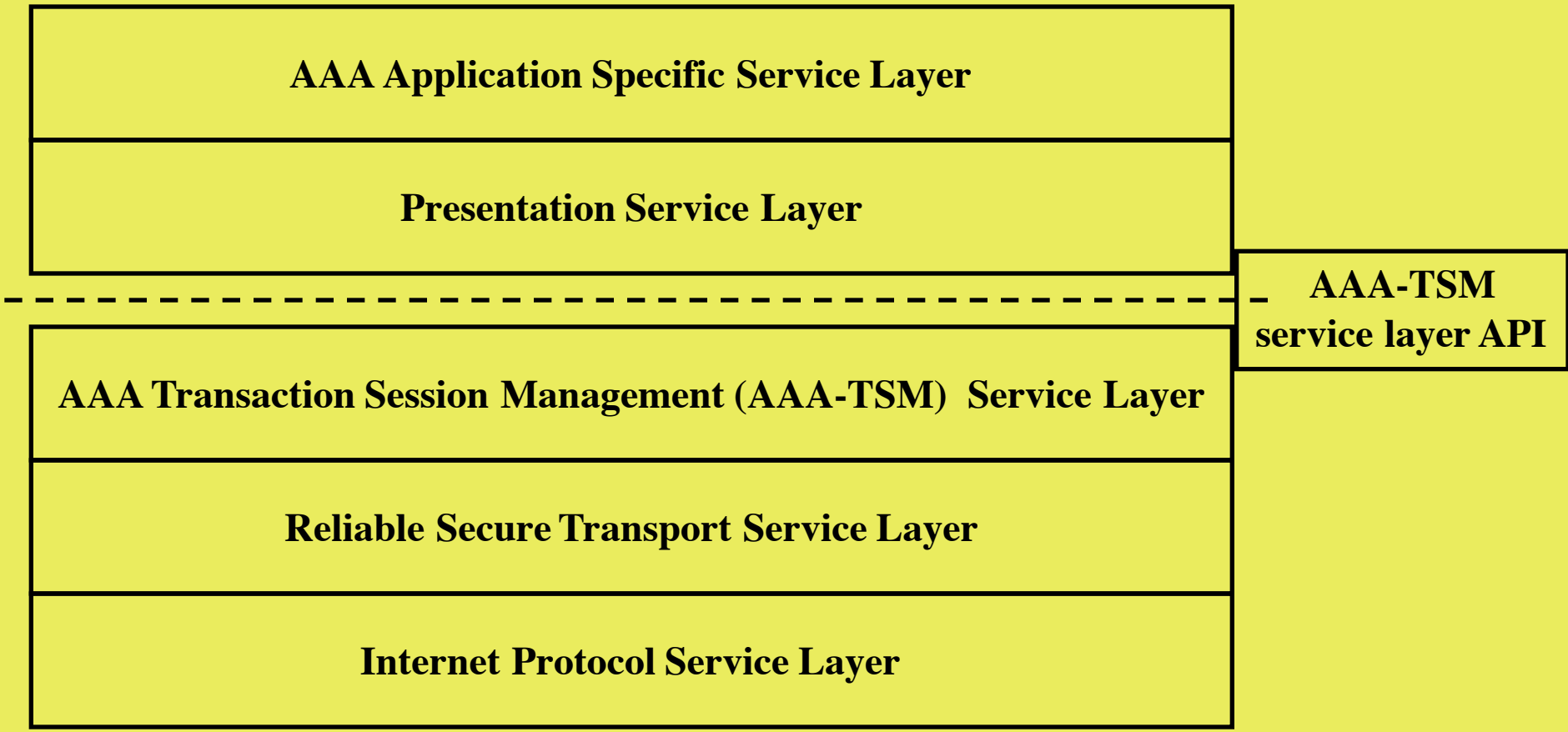
Distributed Authorization Decision Making

- An authorization request must be routed amongst one or more authorization stakeholders
- Each stakeholder executes an Authorization Decision Function (ADF) to approve, deny, or conditionally approve the request
- The authorization request accumulates approvals and other context state information as it passes through the stakeholder chain
- Final approval causes an authorization commit notification to be sent to all of the stakeholders

Post approval: an Authorized Session

- Some authorization request types have no ongoing state after they have been granted, they are transactions
- But there are many authorization types that cause an allocation and ongoing service/resource consumption
- Implies requirements for:
  - monitor session's service/resource use against limits
  - coordinate Authorized Session state across AAA servers
  - network operator interface to view, modify, or cancel session
  - an option for User to modify session's current authorization
- These requirements are met by the AAA Server's resource manager component

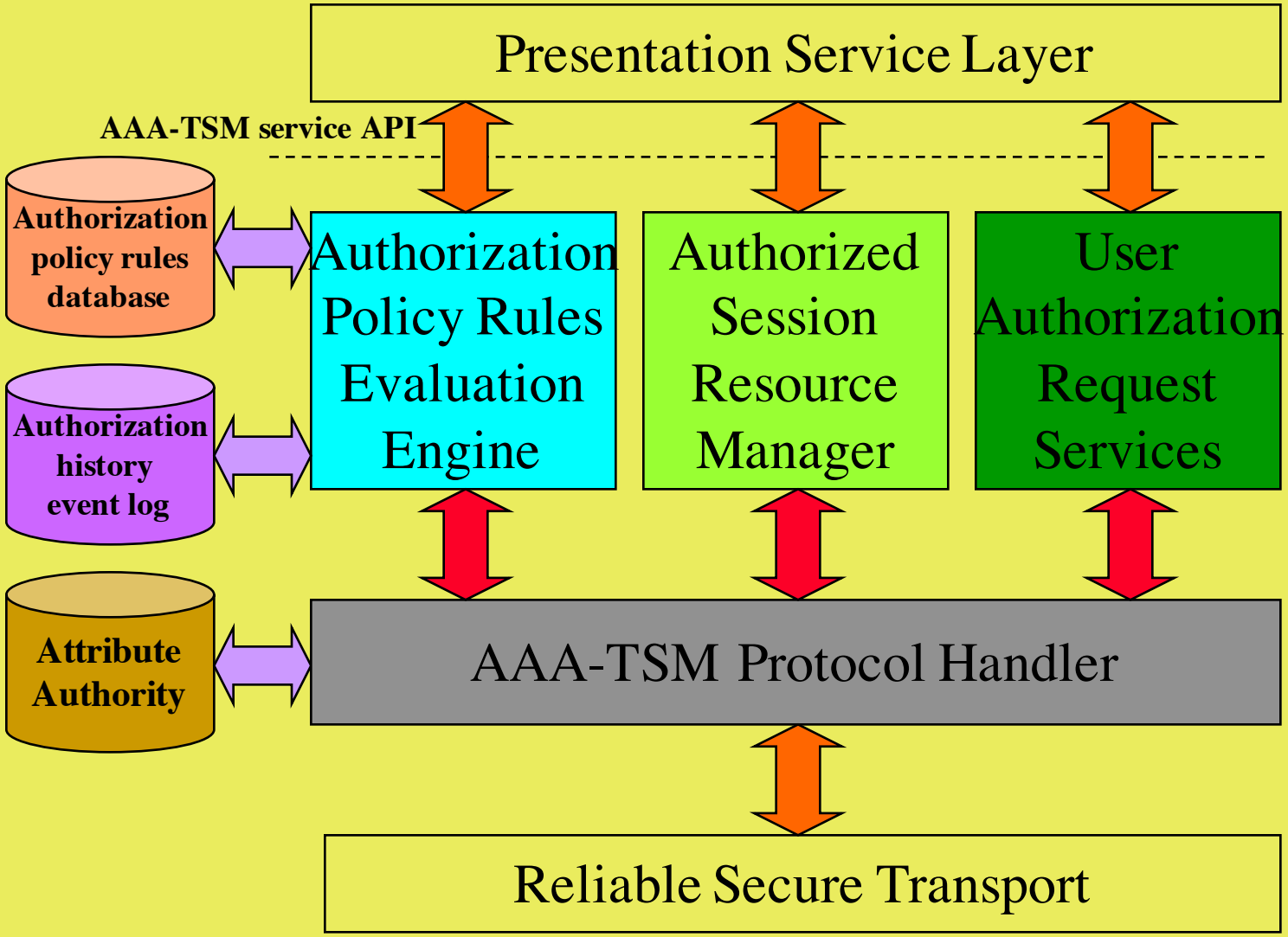
AAA Server Protocol Stack



Service Layer Components

- Service layer [N] abstract program interface that offers a service to its adjacent service layer [N+1]
- A lexicon of Protocol Data Units (PDU) exchanged between the distributed service layer peers
- Service layer end point address space, by which PDUs are routed to their destination
- Trust relationships between the peer end points
- Service layer end point's externally visible Finite State Machine (FSM) and events that cause transitions
- Mechanisms for end point registration, discovery, detect lost connectivity, service location by search attributes

Generic AAA Server Components



Generic AAA Server Components

- Generic authorization decision function driven by policy rule evaluation engine
- Program interface to one or more Application Specific Modules (ASM)
- Authorization history event log - can be consulted by ADF, or used for auditing
- Generic authorization policy rule repository
- Authorized Session resource manager - control point for querying, canceling, or modifying in progress authorized sessions

AAA-TSM Request Payload

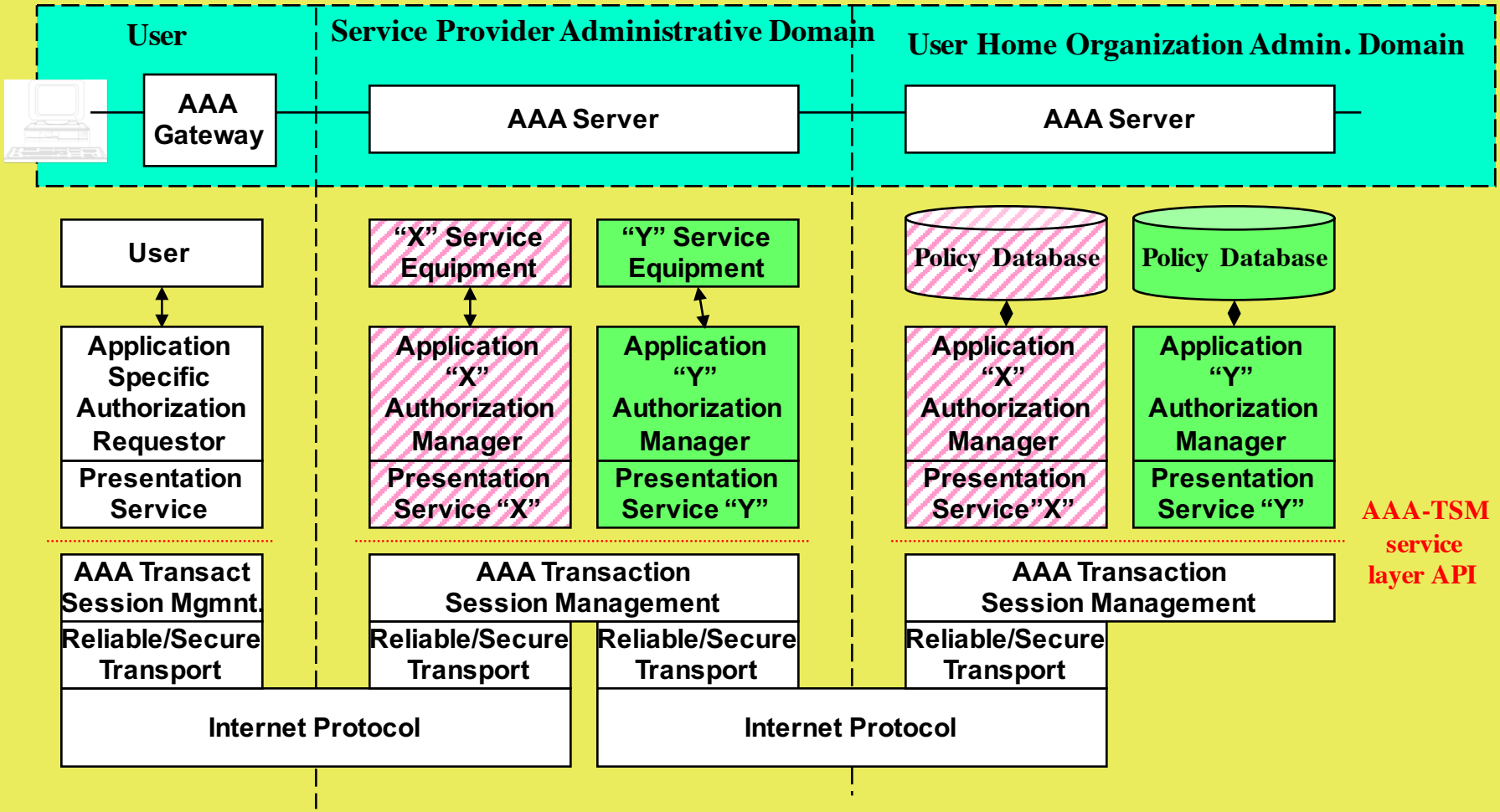
AAA-TSM Request

- AAA-TSM Common Header
- User's Authorization Request
- Authorization Stakeholder Routing List
- User's credentials, e.g.attribute certificate
- User's identity
- Authorization Completed Approvals List
- Payload Modification Audit Trail
- Authorization formula partial results stack

Completed Approval List Member

- Authorizer's Session Layer Address
- Authorizer's approval digital signature
- Application-specific response data
- Authorizer's decision serial number
- Generic decision status code
- Timestamp of decision

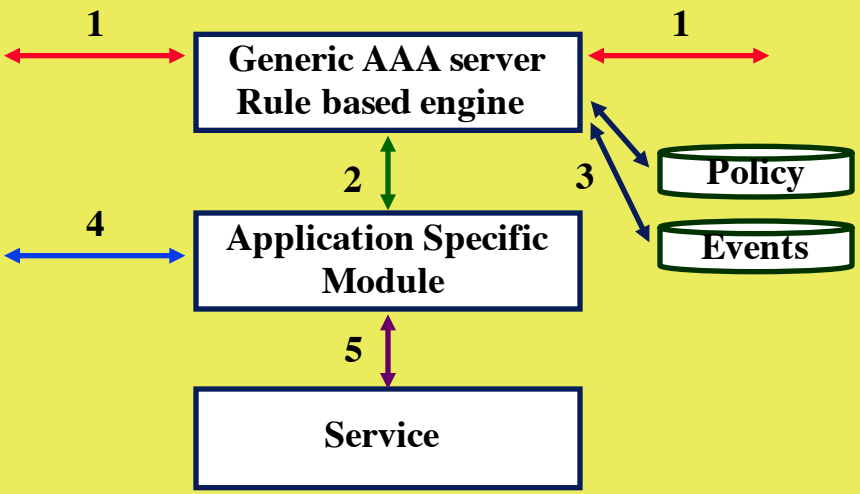
AAA Protocol Stack - end to end view



This scenario shows the User requesting an authorization transaction that requires getting approval from both of two AAA applications, X and Y

Future work

- Define exactly what goes in which component
- Determine what needs to be standardized
  - Type 1 protocol
  - Naming space (what needs to be globally addressable)
  - Policy and rule language(s) (Policy Framework WG)
  - Audit overview
  - Management
- Discrete event simulation
  - Try implementation of simple rules
  - Scalability
  - Looping rules (PF-WG)
    - » A says yes if B says yes and B says yes if A says yes
  - Try simple naming schemes and (re)routing (URL-like???)



Questions to the WG

- Does this work create a base for completing a "generic architecture" for future A³(A) work?
- Should the results in this work be reflected in the new charter for this group?

Current charter wording -->

Collecting and satisfying application-layer requirements is not in the current set of AAA WG milestones. However, if a set of agreed upon application-layer requirements can be delivered before the deadline of I-D submission for the next IETF, then such document(s) will/may be considered.

We propose a revision!

Proposed New Charter Items

- Develop Generic AAA Model by explicitly including Authentication and Accounting
- Develop model for management of a WEB of AAA-Servers
- Develop auditability framework specification
- Align development for short term AAA protocol to be fitting in long term AAA model
- Tackle interdomain issues using the proposed generic model

Proposal:

Advance current generic authorization model draft to AAA-WG info RFC