IRTF-RG
Authentication Authorisation and Accounting ARCHitecture

chairs:
C. de Laat
J. Vollbrecht
• **Applications**
  
  – Network Access
  – Bandwidth Broker
  – Authorization of resources living in many administrative domains
  – Budget system
  – Library system
  – Computer based education system
  – E-Commerce
  – Micro-payments
  – Car Rental
  – Daily life
Physics-UU to IPP-FZJ => 7 kingdoms

- Physics dept
- Campus network
- SURFnet
- TEN 155
- WINS/DFN
- Juelich, Campus
- Plasma Physics
The need for AAA

Kingdom N

End user

Remote service

Kingdom N+1

AAA

BB

management

R

R

AAA

BB

management

R

R

$$$

The need for AAA

End user

Remote service

Kingdom N

Kingdom N+1

AAA

BB

management

R

R

AAA

BB

management

R

R

$$$
Applications

- PPP Dialin with Roaming (Network Access)
- Mobile-IP
- Bandwidth Broker
- Internet Printing
- Electronic Commerce
- Computer Based Education and Distance Learning

• Requirements

- Take high level requirements from the different applications as notified in the AAA drafts
- Separate common from application specific functionality
- Authorization of resources living in many administrative domains
AAA Server building block

Rule example: \text{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)
Types of communication:
5: Towards service (f.e. COPS, CLI, SNMPv3)
Generic AAA server
Rule based engine

Application specific Module

Policy
Events

Types of communication:
4: Legacy protocols (Radius, Diameter, …)
• We will now examine the generic AAA problem from the perspective of a layered protocol model
• This contribution is mostly done by George Gross
Roaming “Pull” Authorization Model

Example applications: Mobile IP, PPP dial-in to NAS
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
AAA Server Protocol Stack

- AAA Application Specific Service Layer
- Presentation Service Layer
- AAA Transaction Session Management (AAA-TSM) Service Layer
- Reliable Secure Transport Service Layer
- Internet Protocol Service Layer

AAA-TSM service layer API
Generic AAA Server Components

Presentation Service Layer


Authorized Session Resource Manager

User Authorization Request Services

AAA-TSM service API

AAA-TSM Protocol Handler

Reliable Secure Transport

Authorization policy rules database

Authorization history event log

Attribute Authority
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
This scenario shows the User requesting an authorization transaction that requires getting approval from both of two AAA applications, X and Y.
The architecture's focus is to support AAA services that:

- can inter-operate across organizational boundaries
- are extensible yet common across a wide variety of Internet services
- enables a concept of an AAA transaction spanning many stakeholders
- provides application independent session management mechanisms
- contains strong security mechanisms that be tuned to local policies
- is a scalable to the size of the global Internet
Specific goals of the RG are:

- develop generic AAA model by specifically including Authentication and Accounting
- develop auditability framework specification that allows the AAA system functions to be checked in a multi-organization environment
- develop a model that supports management of a "mesh" of interconnected AAA Servers
- define distributed policy framework, coordinate with policy framework WG and others
- develop an accounting model that allows authorization to define the type of accounting processing required for each session
Specific goals of the RG are:

- implement a simulation model that allows experimentation with the proposed architectural models (also work on an emulation)
- describe interdomain issues using generic model
- work with AAA WG to align short term AAA protocol requirements with long term requirements as much as possible
- complete the work in Q3 - 2000 (ambitious)
• **Research Group Name:** AAAARCH

• **Chair(s)**
  - John Vollbrecht -- jrv@merit.edu
  - Cees de Laat -- delaat@phys.uu.nl

• **Mailing list(s)**
  - aaaarch@fokus.gmd.de
  - For subscription to the mailing list, send e-mail to majordomo@fokus.gmd.de with content of message subscribe aaaarch end
  - will be archived, retrieval with frames
    » http://www.fokus.gmd.de/glone/research/aaaarch/
  - in plain ascii:
    » http://www.fokus.gmd.de/glone/research/mail-archive/aaaarch-current
    » ftp://ftp.fokus.gmd.de/pub/glone/mail-archive/aaaarch-current

• **Web page**
  - Http://www.phys.uu.nl/~wwwfi/aaaarch