Akogrimo Training Event, December 12, 2005, Madrid, Spain

Akogrimo's A4C Component

Cristian Morariu[1], Peter Racz[1], David Hausheer[1], Laura de Pablo[1], Burkhard Stiller[1,2]
[1] Communication Systems Group CSG, Department of Informatics IFI, University of Zürich
Winterthurerstrasse 190, CH-8057 Zürich, Switzerland
and
[2] Computer Engineering and Networks Laboratory TIK, ETH Zürich
Gloriastrasse 35, CH-8092 Zürich, Switzerland
[morariu¦racz¦hausheer¦depablo¦stiller]@ifi.unizh.ch

Overview and A4C Challenges
A4C Scenario and Process
Design and Architecture
Implementation and Summary

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Project Overview

- Akogrimo:
  - Blueprint and architecture for a NGG
  - Mobile Internet and IPv6
- A4C (Authentication, Authorization, Accounting, Auditing, and Charging):
  - Personalized access to services “everywhere, anytime using any type of access”
  - Appropriate security models for Virtual Organizations
  - Creation and management of dynamic trust domains
  - Support for revenue generation
  - Unified billing

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Introduction

- Separated world of network services and grid services:
  - Goal to integrate networking and grid views of services for A4C purposes into a single, logical component
  - DIAMETER–based AAA solution
    - Enhanced with Auditing and Charging capabilities
    - Enhanced with grid-specific Attribute-Value-Pairs (AVP)
- Thus, A4C support will be offered to a larger set of services than traditional network services

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

A4C Challenges (1)

Authentication and Authorization

- Single *Sign-On*
- Delegation
- Integration with local security solutions
- User-based trust relationship
- Communication protection
- Manageability:
  - Identity management
  - Policy management
  - Key management

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

A4C Challenges (2)

Accounting and Auditing

- Define parameters to be metered and accounted for
- Secure logging of audit information
- Intrusion Detection Systems (limited view within Akogrimo)

Charging and Pricing

- Define parameters to be charged for
- Integrate multiple pricing schemes from different players
- Unified Billing
  - Grid services and network transport

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Related Work and Background: RADIUS and Diameter Overview

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

RADIUS

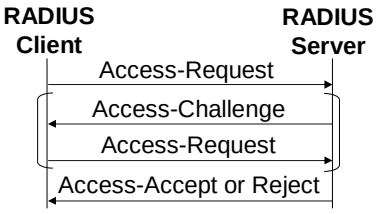
Remote Authentication Dial In User Service (RADIUS)

- Protocol supporting authentication, authorization and accounting
  - RFC 2865
  - RFC 2866
- Widespread deployment in current networks
- Based on client-server model
  - Server can act as a client (proxy)
- UDP is used as transport protocol
- Uses Attribute-Length-Value 3-tuples as representation format
  - Ability to define new attributes and to create vendor-specific extensions
- Applies the hop-to-hop security model

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

RADIUS

- Access control (AA) messages
  - Access-Request
  - Access-Accept
  - Access-Reject
  - Access-Challenge



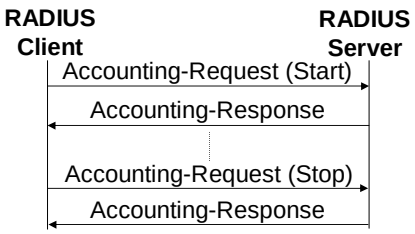
- Attribute-Length-Value
  - Value Types: Integer, Text String, IP Address, Date, Binary
  - Format:

Attribute Number	Attribute Length	Attribute Value

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

RADIUS Accounting

- Accounting messages
  - Accounting-Request
    - Start
    - Stop
    - Interim-Update
  - Accounting-Response



- Accounting specific attributes (examples)
  - Acct-Session-Time
  - Acct-Input-Octets, Acct-Output-Octets
  - Acct-Input-Packets, Acct-Output-Packets
  - Acct-Session-ID
  - Acct-Terminate-Cause

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Diameter

- Diameter is an AAA protocol
  - RFC 3588
  - Fulfils the minimum requirements defined in RFC 2989
  - Successor of RADIUS
- Designed to overcome the deficiencies of RADIUS
  - Different access technologies
  - Distributed security model
  - Multi-domain roaming scenarios
  - Server-initiated messages
  - Better error handling and reporting
  - Capability negotiation
  - Peer discovery and configuration

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Diameter Base Protocol (1)

- Diameter base protocol
  - Defines Diameter entities and specifies the message format
  - Common functionalities
    - Message transport and capability negotiation
    - Error handling and security functions
- Support of different kind of agents
  - Proxy agent, Redirect agent, Relay agent, Translation agent
- Reliable transport
  - over TCP or SCTP
- Security support
  - Hop-by-hop and end-to-end security
  - Support of IPSec and TLS

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Diameter Base Protocol (2)

- Attribute-value pairs (AVPs) for data exchange
  - Extended data formats for AVP data types
  - Standardized set of AVPs is defined
  - Flexible for further extensions
  - AVP format:

AVP Code	AVP Flags	AVP Length	Vendor-ID (optional)	Data

- Diameter accounting
  - Accounting-Request and Accounting-Answer messages
  - Different accounting Record types
    - Event / Start / Interim / Stop record
  - Diameter applications define additional accounting attributes

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Diameter Applications

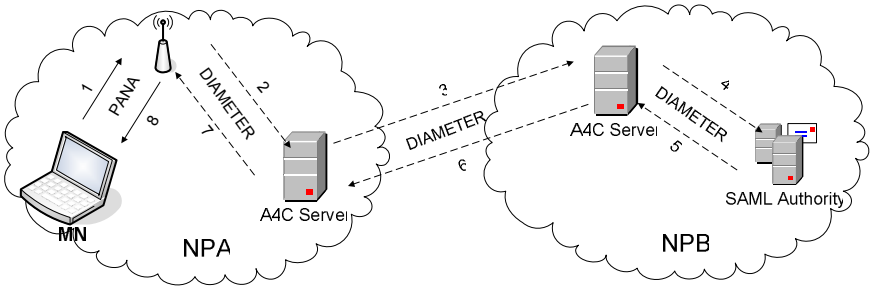
- Service-specific extensions for Diameter
  - Enable a flexible extension of the protocol
  - Define service specific commands and attributes
- Current applications include
  - Network Access Server application
  - Extensible Authentication Protocol (EAP) application
  - Mobile IPv4 application
  - Credit-control application

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Akogrimo A4C Scenarios and Process

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

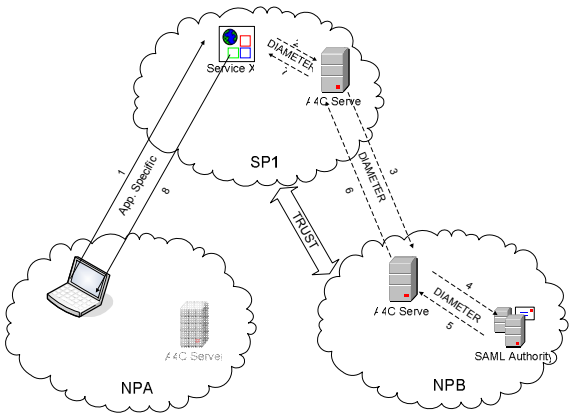
Akogrimo A4C Scenario – Authentication



- MN is in the foreign access network of NPA
- NPA will contact NPB (home domain of MN) for authentication
- NPB will issue an SAML token for proving authentication of MN

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Akogrimo A4C Scenario – Authorization



After authentication MN requests Service X from another SP

1. Service req. containing SAML token

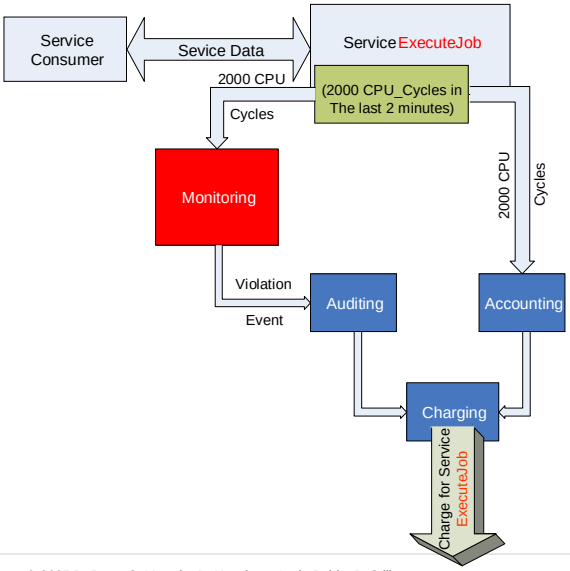
2-6. SP1 checks with NPB validity of the token and retrieves User Profile

7. A4C server of SP1 takes local authorization decision

8. Service delivered to the user

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Accounting and Charging Process



- Every service needs to implement a **meter** for the parameters it wishes to account for
- The meter will feed the **accounting** and monitoring (external to A4C) components
- All the accounting records and audited events generated in a service session will be fed to the charging component
- According to the charging scheme the service charge is calculated and added to a user's monthly bill

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

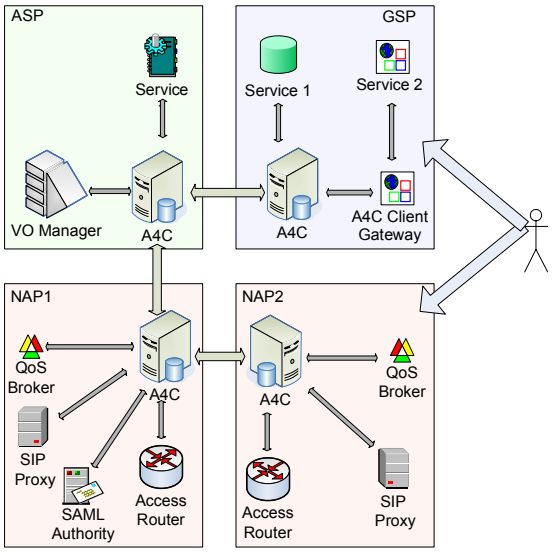
ifi

Akogrimo's A4C: Design and Architecture

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

ifi

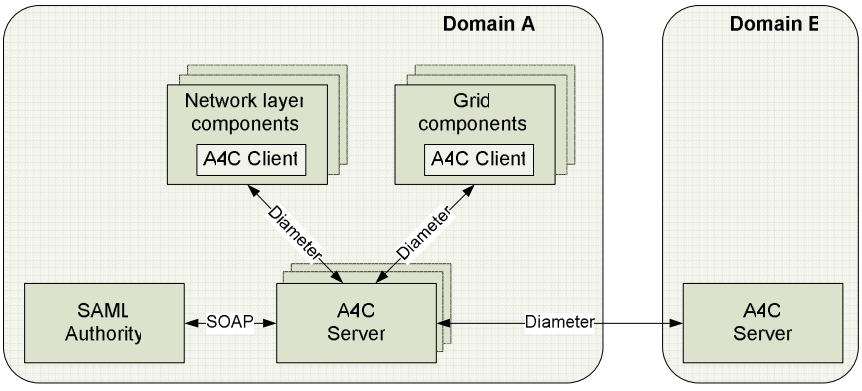
Simplified Network Architecture



- ASP:
  Application Service Provider
- GSP:
  Grid Service Provider
- NAP:
  Network Access Provider

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

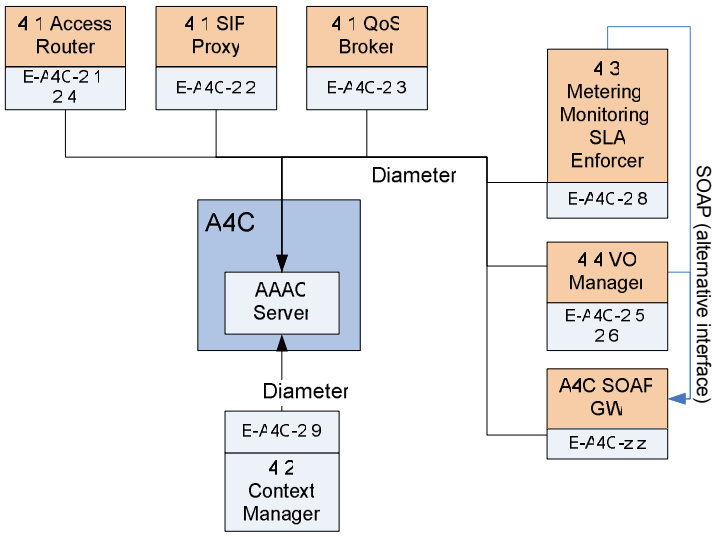
A4C Infrastructure



- Provide A4C services to Grid and Network Components
- Manage the A4C services in a multi-domain environment
- Based on defined IETF standards

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

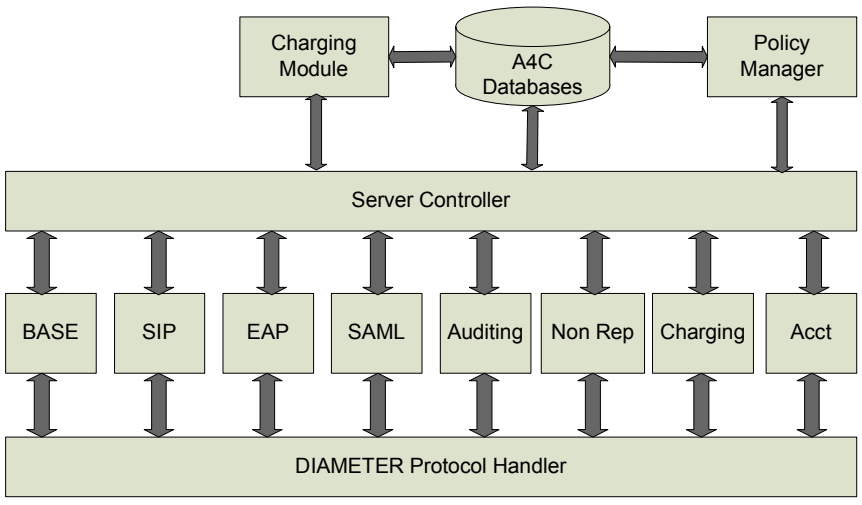
A4C Interfaces to Other Components



- Each component incorporates an A4C Client
- Communication based on
- DIAMETER
- Alternative SOAP interface possible

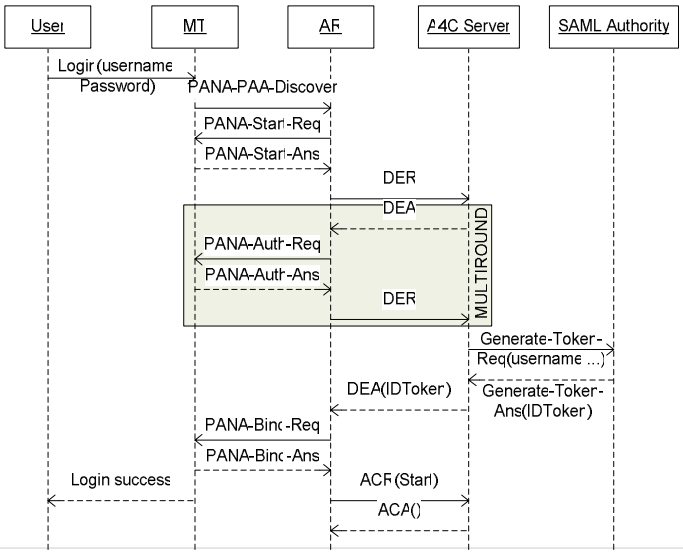
© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

A4C Server Internal Architecture



© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

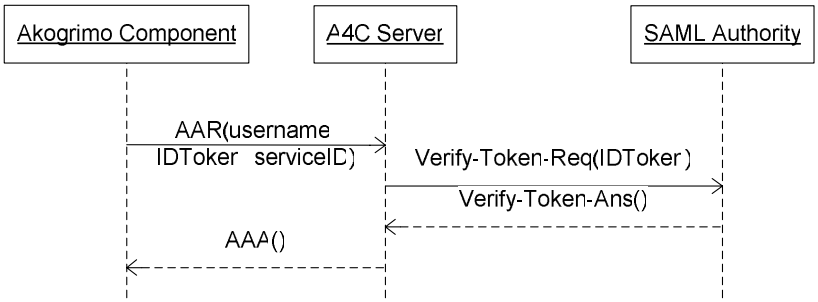
A4C-based Network Authentication



- Network Authentication based on network standards (PANA, EAP, Diameter)
- SAML Integration to support Single-Sign-On
- The IDToken will be used as a proof of authentication

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

A4C-based Authentication Verification



- Used by grid components
- The actual verification is done by the SAML authority which generated the token
- Used when a service is requested
- The user profile can also be sent back after a successful authentication

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Grid and Network Accounting Extensions

- CPU-Time, CPU-Type
- CPU-Cycles, CPU-Count
- Node-Count

- Memory-Size
- Memory-Usage-Average
- Memory-Usage-Maximum

- Disk-Usage-Average
- Disk-Usage-Maximum

- Host-Name, Job-Name
- Process-ID, Process-Status

- QoS-Bandwidth
- QoS-Delay
- QoS-Jitter
- QoS-Priority
- QoS-DSCP
- QoS-Score

- Accounting-Dropped-Octets
- Accounting-Dropped-Packets

- Request-Count
- Successful-Request-Count
- Failed-Request-Count

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

ifi

A4C Implementation

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

ifi

Implementation Components

- A4C Server
  - Based on OpenDiameter framework
  - Linux, C++
- A4C Client
  - Linux, C++
  - Java API also available
- Data Storage
  - MySQL database
  - Linux, C++
  - Standalone component
- SAML Authority
  - Java Web-Service

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Software Components and Libraries

- Diameter protocol
  - Opendiameter library v1.0.7-f
- Communication framework
  - ACE library v5.4.1
  - Boost library 1.0.3
- Database
  - MySQL 4.0
  - mysql-connector-java 3.0.15
  - MySQL++ 2.0.5
- XML parser
  - Xerces C++ 2.6.0
- XML security
  - XMLsec v1.1
- Security funtions
  - OpenSSL library
- SAML messages
  - OpenSAML v1.1
- SOAP messages
  - Axis framework v1.2

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Interface Implementation Issue

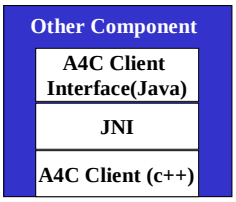
- A4C Client uses “Open diameter library“ written in C++
- Most of Akogrimo components written in Java

→ Need for a Java-based A4C Client

Solution

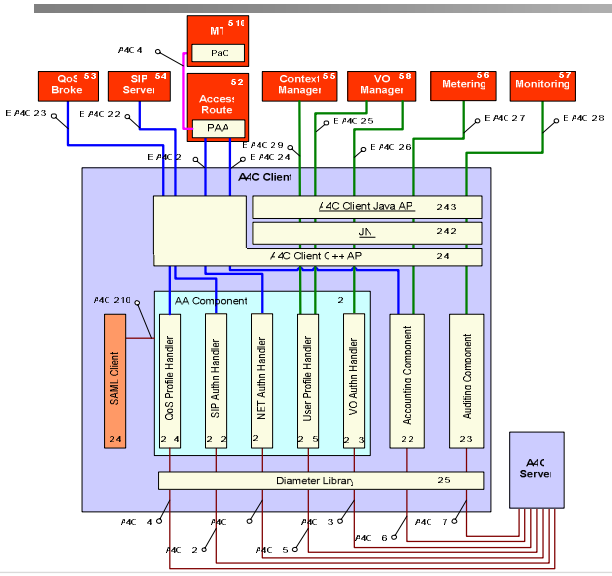
- Use of JNI (Java Native Interface)

→ Enables to access libraries written in C or C++ via Java API



© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

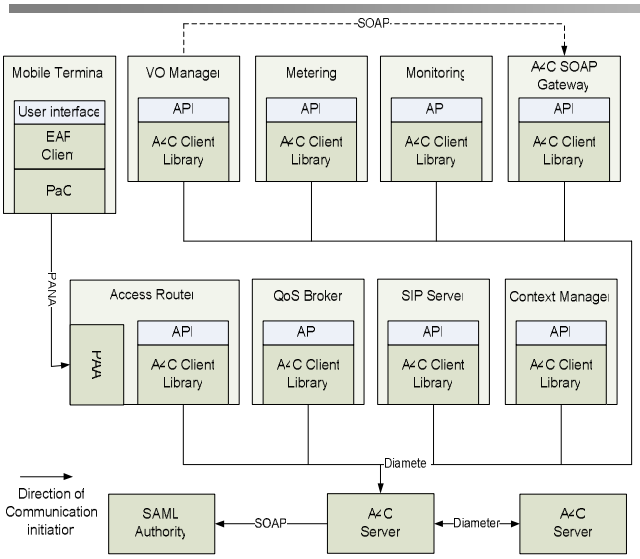
A4C Client Interfaces



- Specialized interfaces for different tasks
- Modular tasks, new functionalities easy to add
- Software interfaces are mapped to DIAMETER commands
- Interfaces offered in C++ and Java

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Deployment



- A4C Server and SAML Authority: standalone servers
- All components acting as A4C clients need to use the A4CClient library
- Special library for the Mobile Terminal offering PANA support

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Accounting API Example

- Create an A4C client

```
A4CClientModule A4Cmodule(clientCfgFile);
```

- When a new service session is started, we need to start a new accounting session

```
sessionID = A4Cmodule.accountingSessionStart(userName,
   serviceId);
```

- Create and send an accounting record

```
AccountingRecord Record =
   A4Cmodule.createAccountingRecord(sessionId);
Record.addAVP(avpID, avpValue);
A4Cmodule.sendAccountingRecord(sessionID, Record);
```

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Charging Specification Format

- Defines the rules and prices to be applied for charging
- Enables user, service, and domain-specific tariffs

- Defined in XML format
- Generic format of the charge calculation:

$$C_S = P_S + \sum_i T_i$$

$$T_i = \prod_k AVP_k \cdot P$$

C_S: session charge

P_S: service price

T_i: term

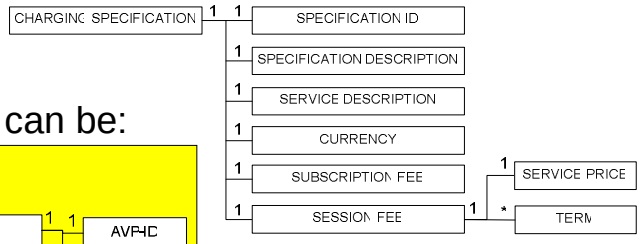
AVP_k: a particular accounting attribute (AVP)

P: a particular price for the term

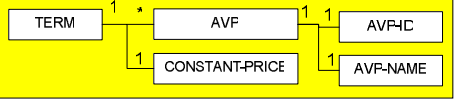
© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Charging Specification Format

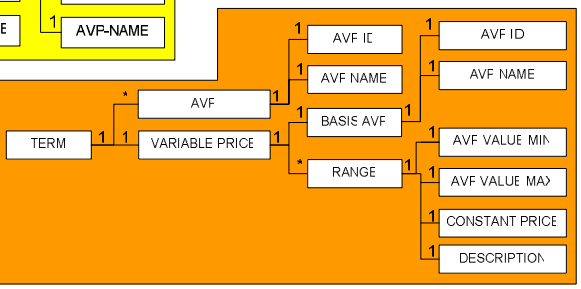
- XML structure



- The applied price can be:
  - Constant



  - Variable depending on a value of a particular AVP

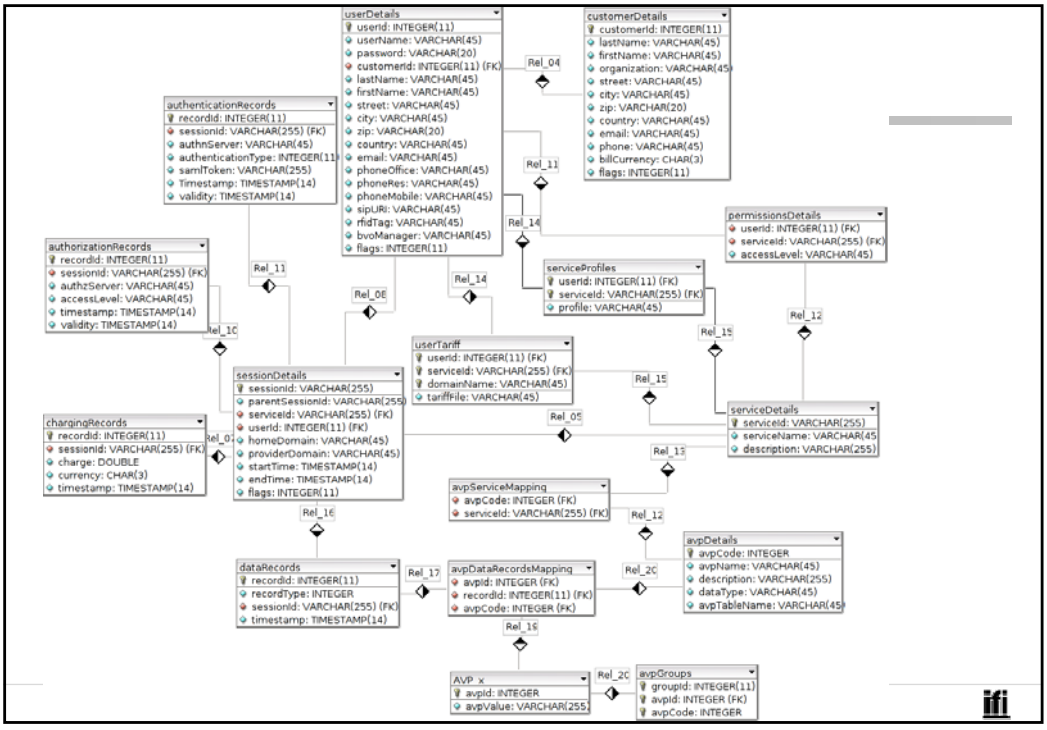


© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Charging Specification Format (Example)

```
<?xml version="1.0" encoding="UTF-8"?>
<CHARGING-SPECIFICATION>
   ...
   <CURRENCY>EUR</CURRENCY>
   <SUBSCRIPTION-FEE>9.95</SUBSCRIPTION-FEE>
<SESSION-FEE>
   <SERVICE-PRICE>0.5</SERVICE-PRICE>
   <TERM>
        <AVP> <AVP-ID>46</AVP-ID> <AVP-NAME>Acct-Session-Time</AVP-NAME> </AVP>
        <CONSTANT-PRICE>0.15</CONSTANT-PRICE>
   </TERM>
   <TERM>
        <AVP> <AVP-ID>363</AVP-ID> <AVP-NAME>Accounting-Input-Octets</AVP-NAME> </AVP>
        <VARIABLE-PRICE>
                <BASIS-AVP> <AVP-ID>363</AVP-ID>
                          <AVP-NAME>Accounting-Input-Octets</AVP-NAME>
                </BASIS-AVP>
                <RANGE>  <AVP-VALUE-MIN>0</AVP-VALUE-MIN>
                         <AVP-VALUE-MAX>1000000</AVP-VALUE-MAX>
                         <CONSTANT-PRICE>0.0005</CONSTANT-PRICE>
                </RANGE>
                <RANGE> ... </RANGE>
        </VARIABLE-PRICE>
   </TERM>
</SESSION-FEE>
</CHARGING-SPECIFICATION>
```

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller



Summary

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Summary and Conclusions

- A4C shall ease the merging of the Grid and Networking worlds
- A4C shall support the creation of diverse business processes
  - Supported by offering user access control and resource usage accounting across different administrative domains
- DIAMETER seems the right AAA protocol choice
  - Client implementation in every service is not yet feasible

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller

Future Work

- Integration of grid authorization in A4C
- Exposing of A4C services as web-services
- Virtual Organization awareness not yet present in A4C
- Integration of an charging/billing settlement entity

© 2005 P. Racz, C. Morariu, D. Hausheer, L. de Pablo, B. Stiller