AA-RR:

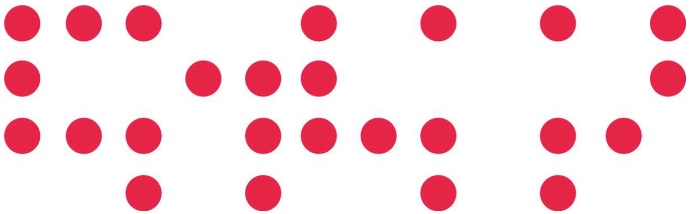
Working with Authentication and Authorization Infrastructures

Ajay Daryanani
Middleware Engineer
RedIRIS/Red.es

Markham, 1st November 2006

RedIRIS

Outline



Background

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

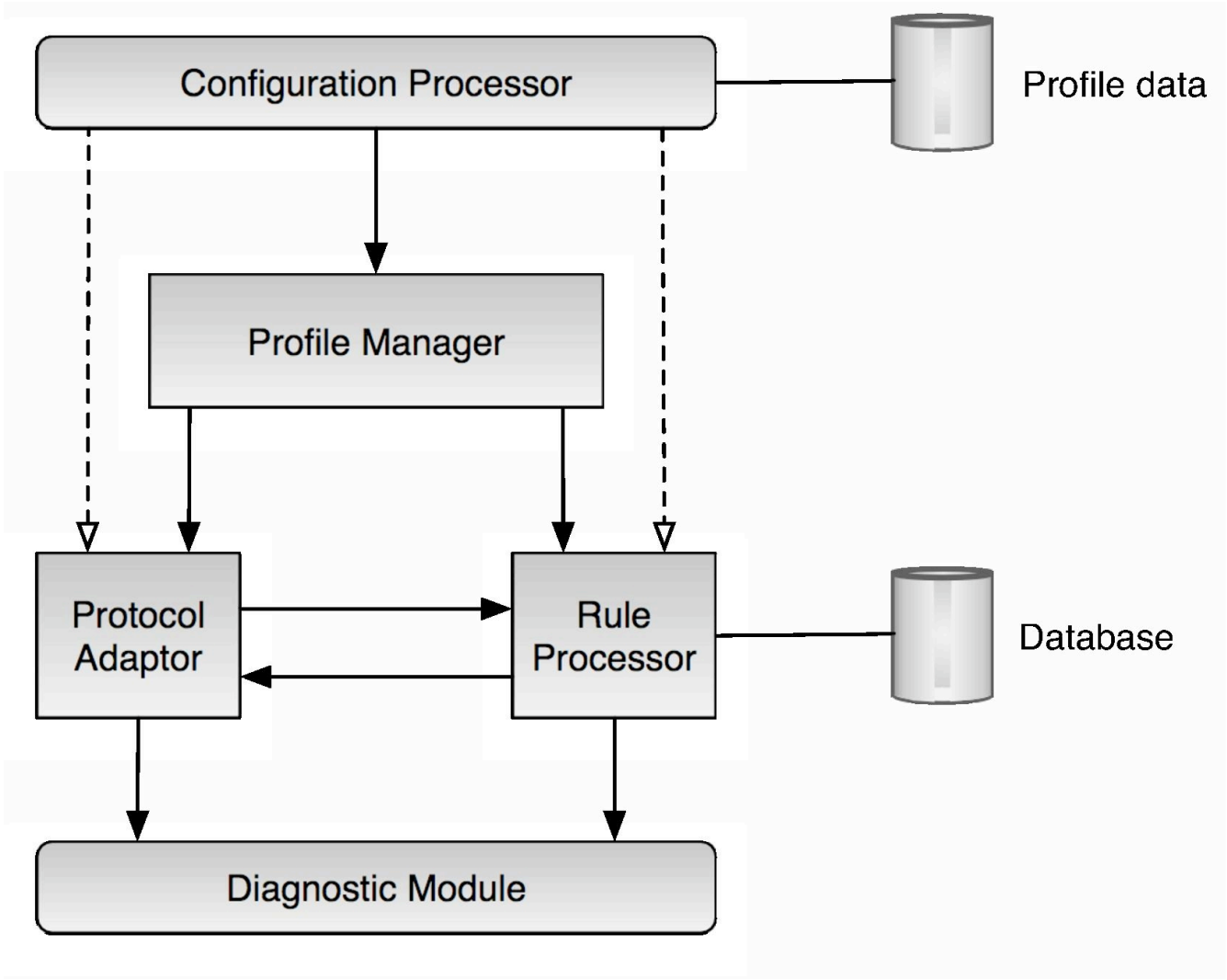
- Growing interest in ID management has led to several different
  - AuthN and AuthR protocols
  - Commercial and open source systems
  - Trust models (federations, confederations)
- Development / integration of AAIs is not straightforward
  - Implies high cost (also in human resources)
  - Lack of validation tools in the community

RedIRIS

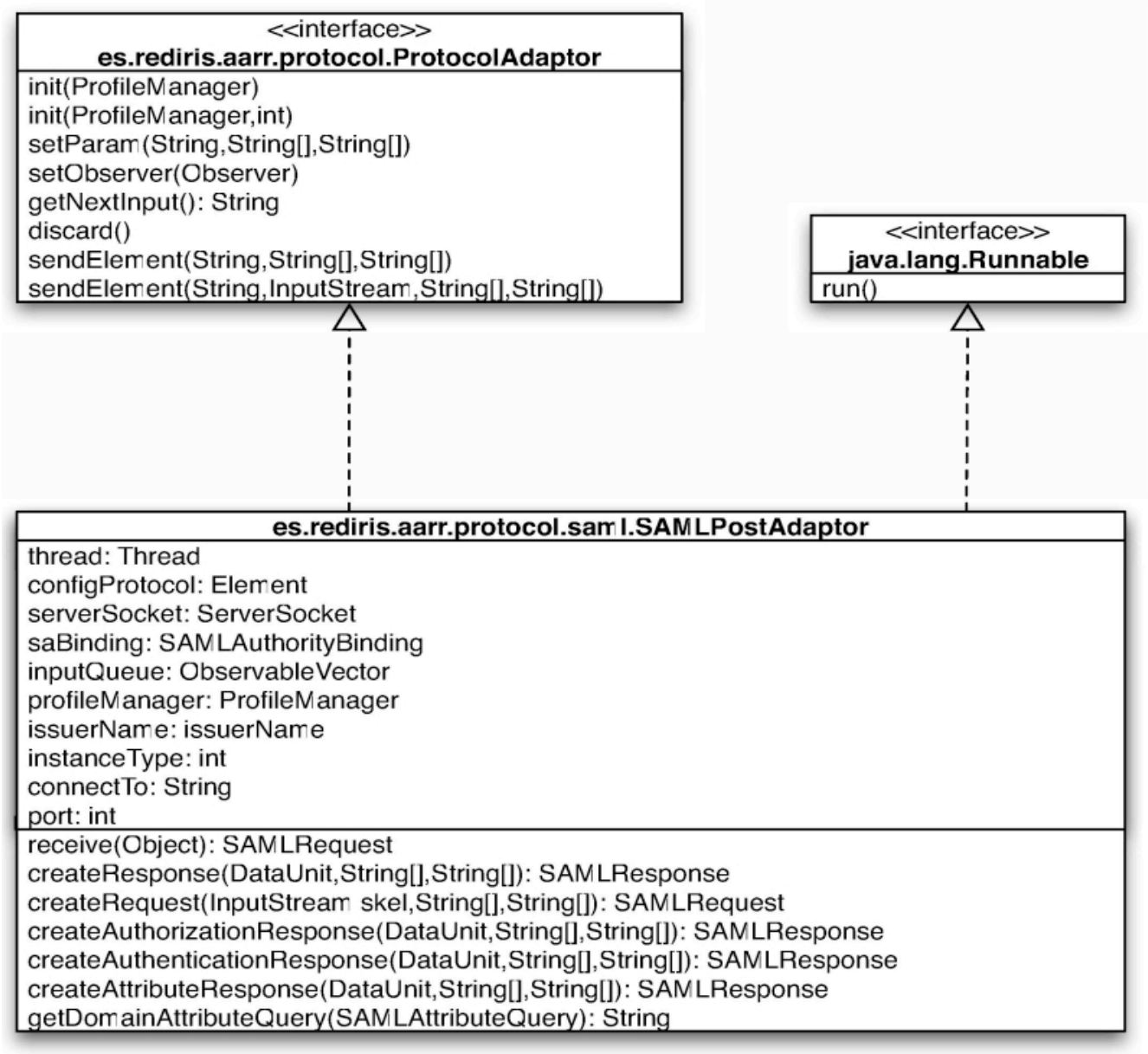
AA-RR Features

- AA-RR is an open source validation tool
  - Able to emulate any AA component
  - Written in Java, using XML configuration files
  - Independent of protocol and communication mechanism
  - Decoupled components => easier adaptation
- Main emulation components
  - Attribute sources
  - Attribute requesters
  - Authorization engines

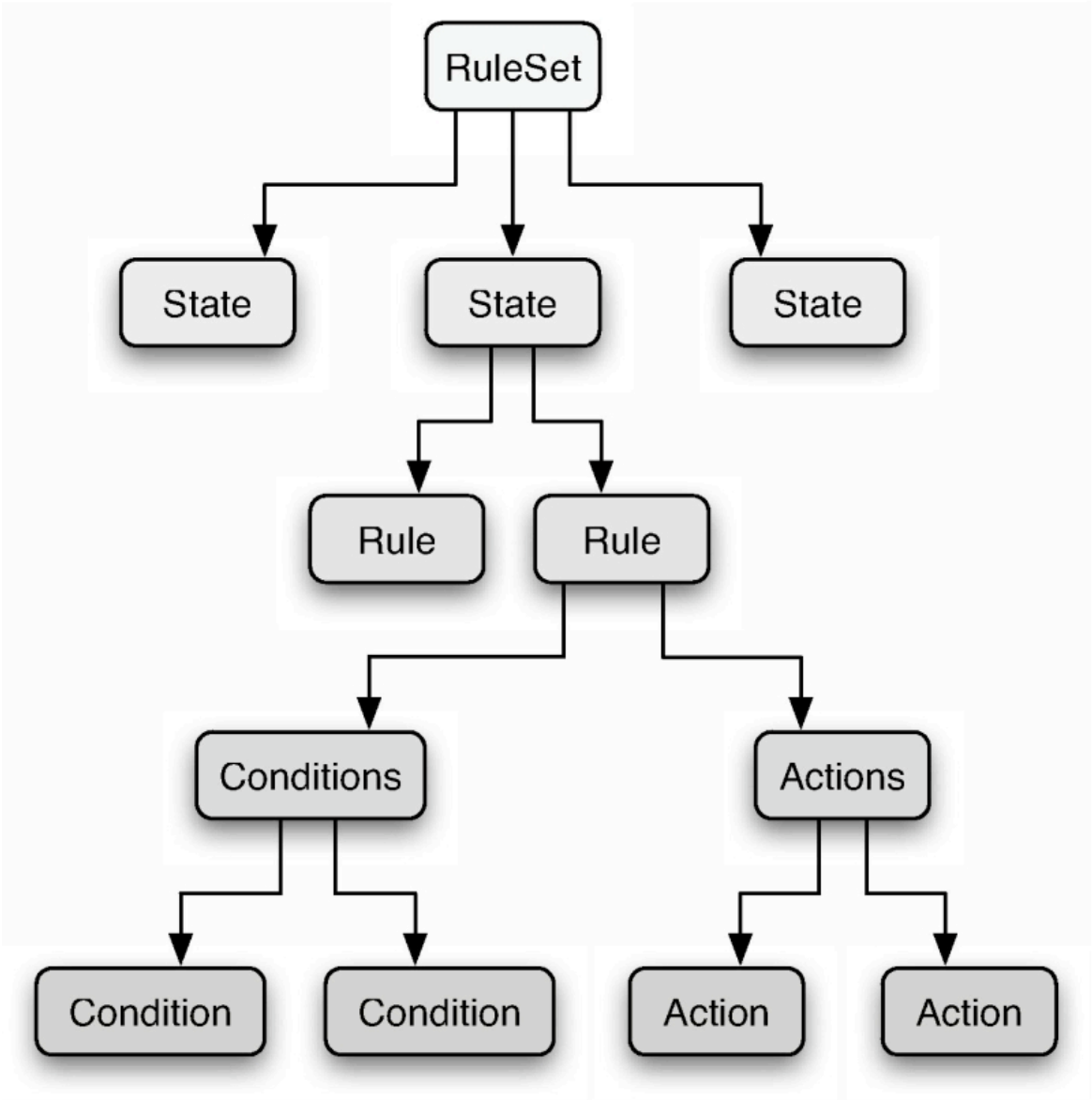
Architecture: Overview



Architecture: Protocol adaptors



Architecture: Rule processors (1)



Architecture: Rule processors (2)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

```
<ruleset name="PAPI-AS_Signed-Query">
 <state name="init">
    <rule name="ATTREQ_Accept">
     <conditions>
      <condition name="received_action" field="ACTION" value="ATTREQ"/>
      <condition name="check_serviceID" field="ValidPoAServiceID" value="true"/>
     </conditions>
     <actions>
      <action name="sent_status" send="Accept">
        <field id="Status" value="ATTREQ_Accept"/>
        <field id="userData" value="user=any,group=any"/>
      </action>
      <action name="next_state" next="finished"/>
     </actions>
    </rule>
 </state>
 <state name="finished">
    <rule name="r1">
     <actions>
      <action name="fp" finish="pass"/>
     </actions>
    </rule>
 </state>
</ruleset>
```

RedIRIS

Applications: HelloSAML

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- http://hellosaml.rediris.es
- An open test site on the Internet to which to test various SAML exchanges (request/response)
- Able to send and respond queries for authentication, authorization or attribute exchange to established services for testing purposes
- Offering access to the logs of all operations performed on behalf of a certain user.
- Around one hundred registered users from academic and industrial environments

RedIRIS

Applications: SAGPoA

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- PAPI is an AAI protocol developed by RedIRIS
  - Components: AS (IdP), PoA (inner SP), GPoA (outer SP)
  - GPoA acts as a trust aggregator for PoAs
  - SAGPoA stands for Stand-Alone GPoA
- Implemented as an AA-RR protocol adaptor
  - With an embedded Web Server
  - AA-RR can be used for operating components, not only testing

RedIRIS

Applications: eduGAIN validation facility

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- eduGAIN is the GÉANT2 Authentication and Authorization Infrastructure
  - "Lays the work ground for interconnecting European academic users with ubiquitous networked services"
- eduGAIN federates federations
  - Provides interoperability between any pair of federations (e.g. Shibboleth-based and PAPI-based)
  - RedIRIS will provide a testing facility by means of an AA-RR protocol adaptor

Acknowledgements

- AA-RR is a project started by Cándido Rodríguez (contact@kan.es) and Diego R. Lopez (drlopez@rediris.es) …
- …teaming up with José Manuel Macías (jmanuel.macias@rediris.es) and Ajay Daryanani (ajay.daryanani@rediris.es)
- We would like to thank
  - TF-EMC2 (TERENA Task Force on European Middleware Coordination and Collaboration)
  - FECYT (Spanish Technology and Science Foundation)
  - CICA (Andalusian Scientific Computer Centre)

AA-RR website:

http://www.rediris.es/app/aarr

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76
www.red.es