Secure Management of Information across multiple Stakeholders

Privacy-preserving Identity Management in SEMIRAMIS

Aljosa Pasic, ATOS

Agenda

- **About SEMIRAMIS**
- **Architecture overview**
- **End-to-end privacy**
- **Use of pseudonyms**

Agenda

- **About SEMIRAMIS**
- **Architecture overview**
- **End-to-end privacy**
- **Use of pseudonyms**

Project Abstract

Secure Management of Information across multiple Stakeholders

- CIP-ICT-PSP.2009.7.1: EU Competitive and Innovation Framework Programme – ICT Policy Support Programme
- Duration: 34 months, March 2010 – December 2012
- Consortium: 9 partners from 6 countries
  - Spain: Atos, University of Murcia, Ceutí City Council
  - Italy: Engineering Ingegneria Informatica, Lecce City Council
  - Germany: Stuttgart University
  - Portugal: Portugal Telecom Inovação
  - Poland: Polska Telefonia Cyfrowa
  - Belgium: European Organisation for Security

- Project coordinator: Atos (charles.bastos@atos.net – Charles Bastos) - Technical coordinator: Stuttgart Univ. (dominik.lamp@rus.uni-stuttgart.de - Dominik Lamp)

Why do YOU need SEMIRAMIS?

- **If you are a citizen in a foreign country you need to:**
  - Use foreign university (FU) services
  - Use foreign telecommunication (FT) services
  - Use foreign healthcare (FH) services
  - In general...use any e-services in a foreign country which would require data (attributes) about you from home country

- **And YOU expect to have access to these services:**
  - Without having to carry your data in paper or electronic form
  - In a seamless and user friendly way
  - In a secure and privacy preserving approach

What SEMIRAMIS can do for YOU?

Scenario "eDOC Services for Citizens" – Use cases

A) Job Hunting
A European Citizen has moved for a period of time to another European country. Once there, the Citizen applies for a job in a Foreign Company .

B) Public Education Access
A Citizen requests the admission for his child at a public education institutio+n in his new destination of residence.

C) Communication Services
A European Citizen has moved for a period of time to another European country, and chooses to have access to a specific Foreign Telco service (e.g. free wifi)

D) Certificate of Residence
A citizen has decided to stay in the Foreign Country and he registers himself in the Foreign City Council.

Scenario "Roaming Student" – Use cases

A) Matriculation
The first process in which the roaming student has to participate when moving to a university in a foreign country is the matriculation.

B) Apply for Courses
After being registered in the Foreign University, the student whishes to apply for courses.

C) Request Communication Services
The student has moved for a period of time to another European country, and chooses to have access to a specific foreign telco services with discounts (e.g. mobile shopping)

D) Economic Aid
A student wants to receive an economic aid from his city council, in this particular case from his Home City Hall.

Circle of trust + central administration = domain

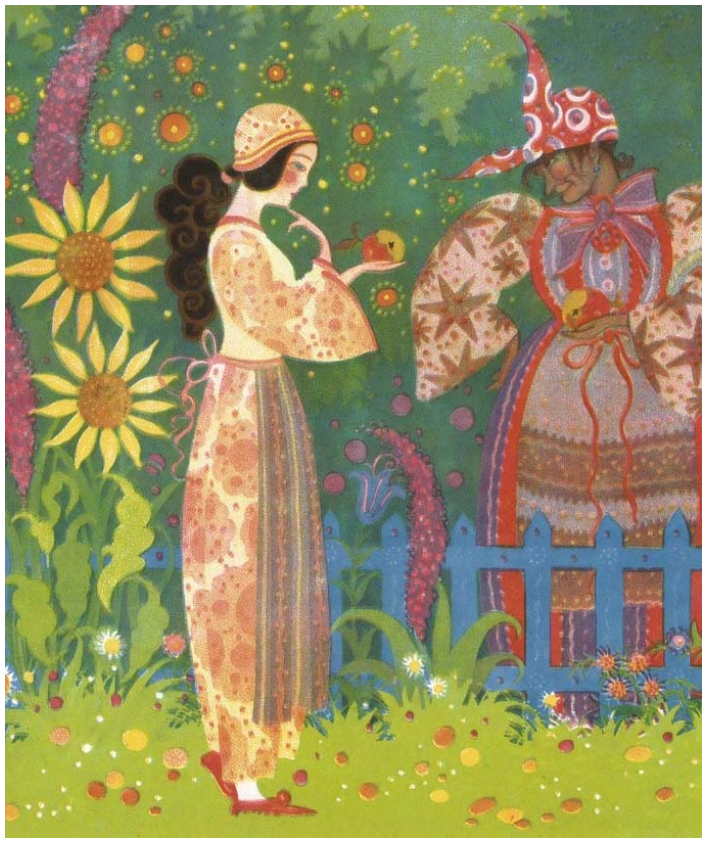
Circle of Trust + dist adm = federation

What are the benefits?

- **Context**
  - Efficient and secure implementation of “cross border” services will become a critical issue for a single European “space”
  - The services span various “circles of trust” – sector or member state specific (public institutions, citizen communities, private institutions)

- **Challenges**
  - Interoperability
  - Usability
  - Efficiency
  - Security, trust between “silos”, and privacy

- **Outcomes**
  - Multi-stakeholder secure and privacy-preserving infrastructure for e-services
    - Data (attribute) and information exchange
    - Open interfaces
    - Modular architecture



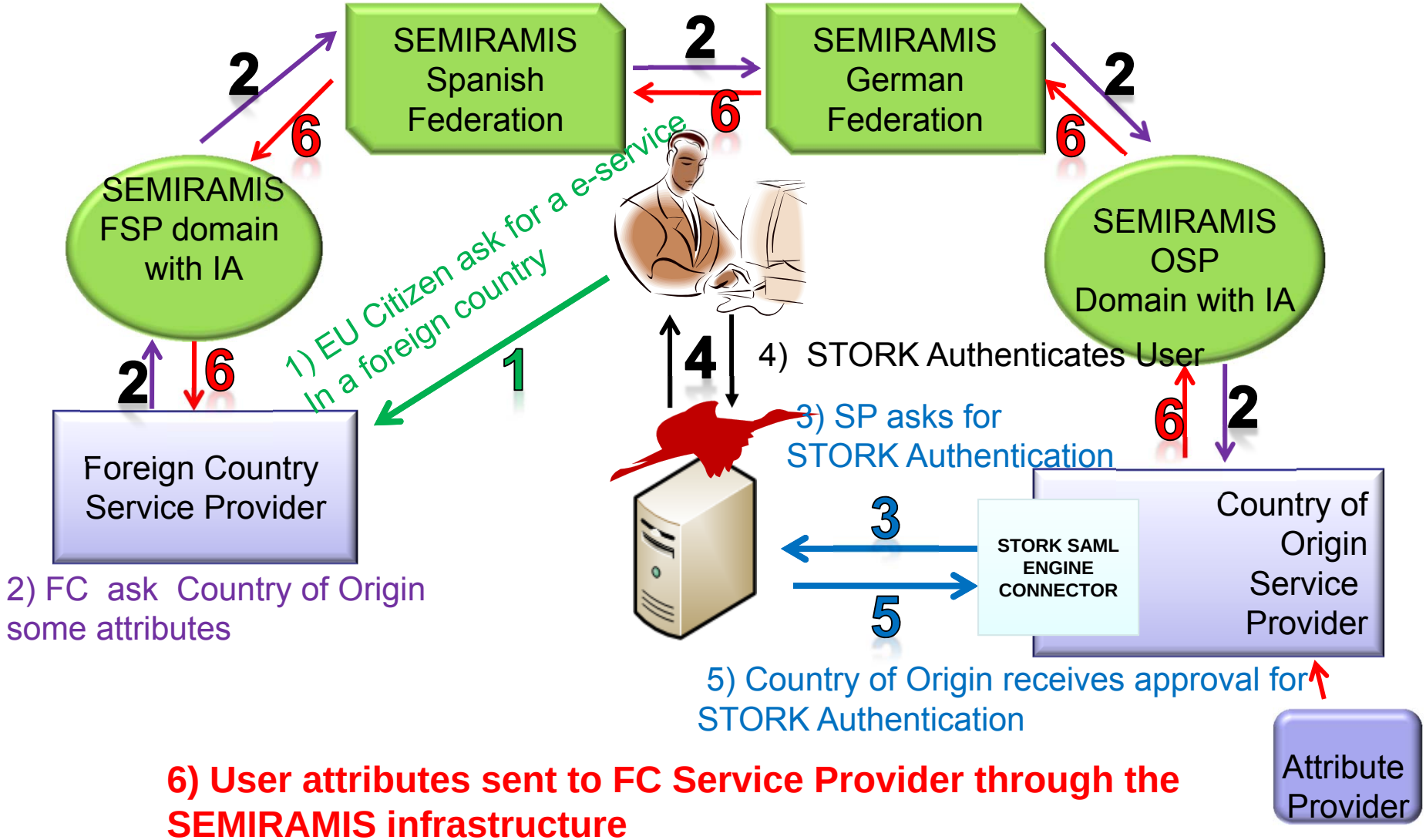
Identity Management

- **Authentication**
  - Web-Authentication
  - Telecommunication Authentication
  - eID Authentication

- **Authorization**
- **Auditing**

- 3 SAML Assertion types (AuthN, AuthZ, Att)
- 2 Protocols: Auth Request, Assertion query/request
- 1 Bindings (to transmit protocol messages): HTTP Post
- Use of SAML extensions: e.g. to avoid re-authentication
- **Several functionalities:**
- **discovery**
- **proxy**
- **translation of attributes**
- **policy config and mngm**
- **routing**
- **forwarding**
- **etc**

SEMIRAMIS at a glance



Attribute aggregation - interoperability

Spain	Portugal	Ital
Last Names	Last Name	Last Name
First Name	First Name	First Name
Date of Birth	Date of Birth	Date of Birth
		Place of Birth
Address		Address (at time
National ID number	National Identification Number	Fiscal Code
Gender		Sex
Nationality		

Form A – Birth certificates
birthDate
birthPlace
name
forenames
sex
father.name
father.forenames

Form B – Marriage certificates
marriageDate
marriagePlace
husband.nameBeforeMarriage
husband.forenames
husband.nameFollowingMarriage
husband.birthDate
husband.birthPlace

SEMIC.EU Core Person
Given Name [0..1]
Family Name [0..1]
Gender [0..1]
Date of Birth [0..1]
Place of Birth [0..1]
Country of Birth [0..1]
Citizenship [0..*]

Name	Description	Type/format
IMSI	The International Mobile Subscriber Identity (IMSI).	Numeric
MSRN	The Mobile Station Roaming Number is a short-lived temporary subscriber identifier. More than one per IMSI could exist.	Numeric
VLR Number	The VLR number is temporary subscriber data and is stored in the HLR. Absence of the VLR number in the HLR indicates that the mobile station is deregistered for non-GPRS or the subscriber does not have a non-GPRS subscription in the HLR.	Numeric
Subscription restriction	Subscription restriction is a parameter indicating whether or not certain restrictions apply to the subscription. The	Structure

Agenda

- About SEMIRAMIS
- Architecture overview
- End-to-end privacy
- Use of pseudonyms

SEMIRAMIS Components

Five core components support the SEMIRAMIS infrastructure.

Identity Aggregator
- Aggregation of eID elements
- Data Protection
- Discovery
- Trust
- Translation

Federation Proxy
- Bridge between federations
- Discovery
- Trust
- Translation
- Interoperability

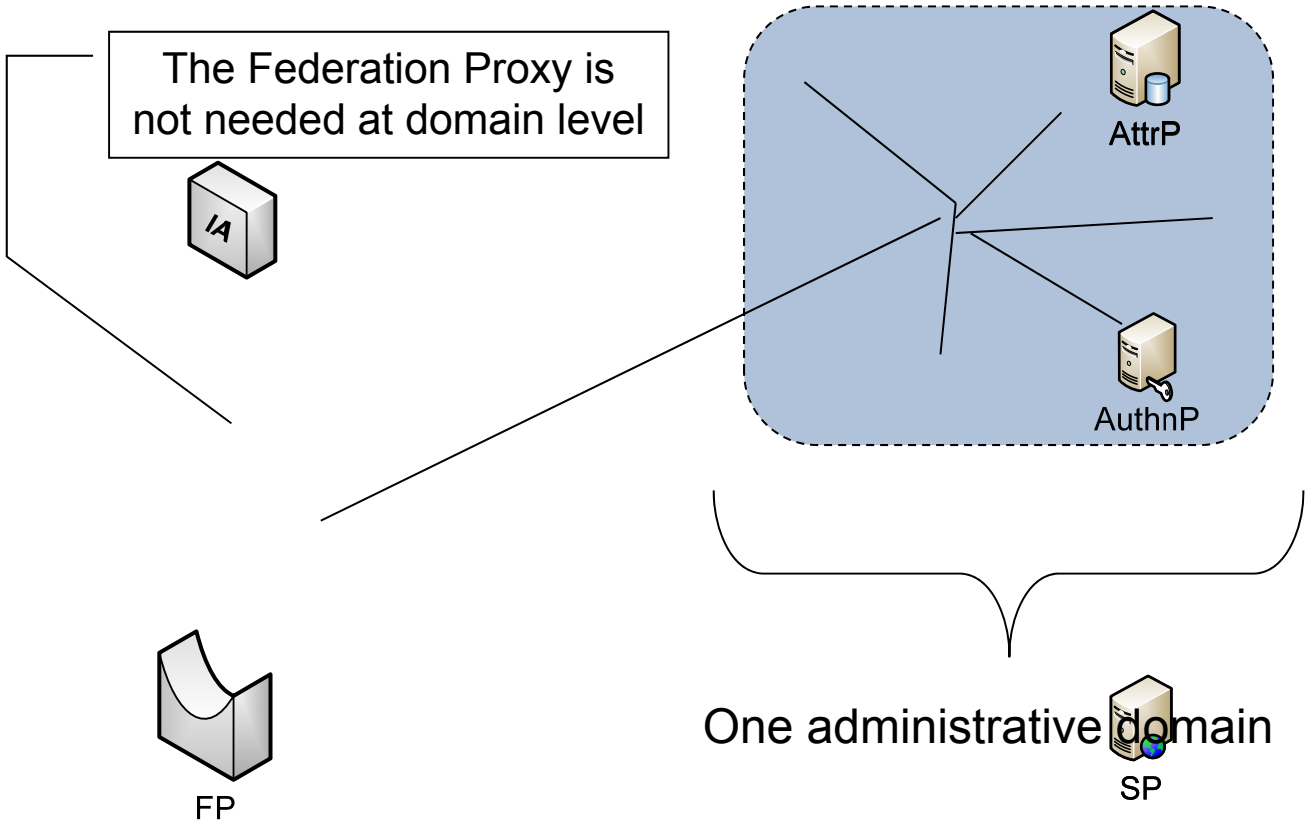
Attribute Provider
- Release Attributes
- Data Protection

Authentication Provider
- User Authentication
- Authentication Validation
- Credential Management

Service Provider
- Provides Services
- Governmental Services
- Academic Services
- Telco Services
- …

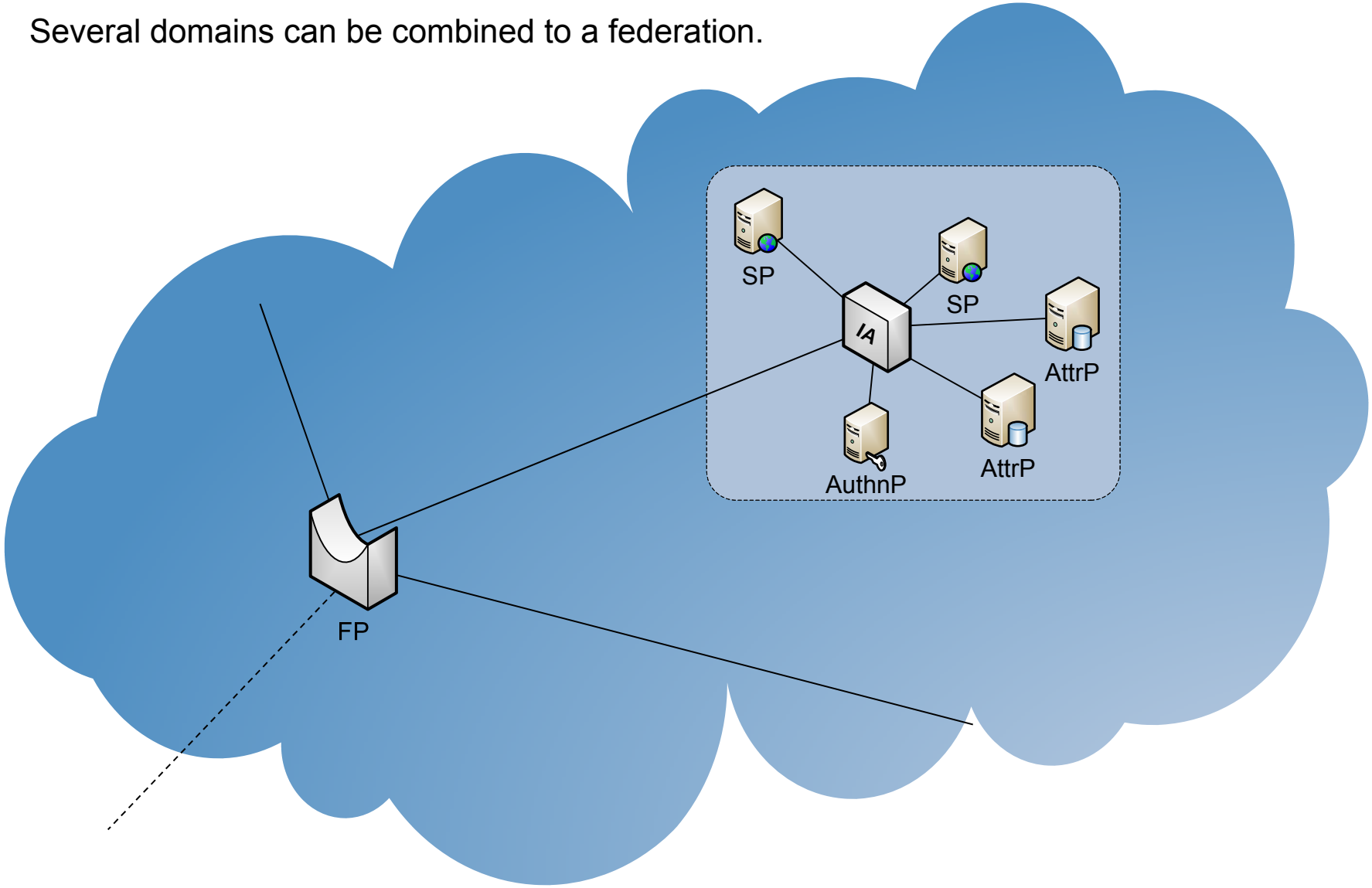
SEMIRAMIS Components - Domain Level

On Domain Level, all components except of the Federation Proxy may be deployed

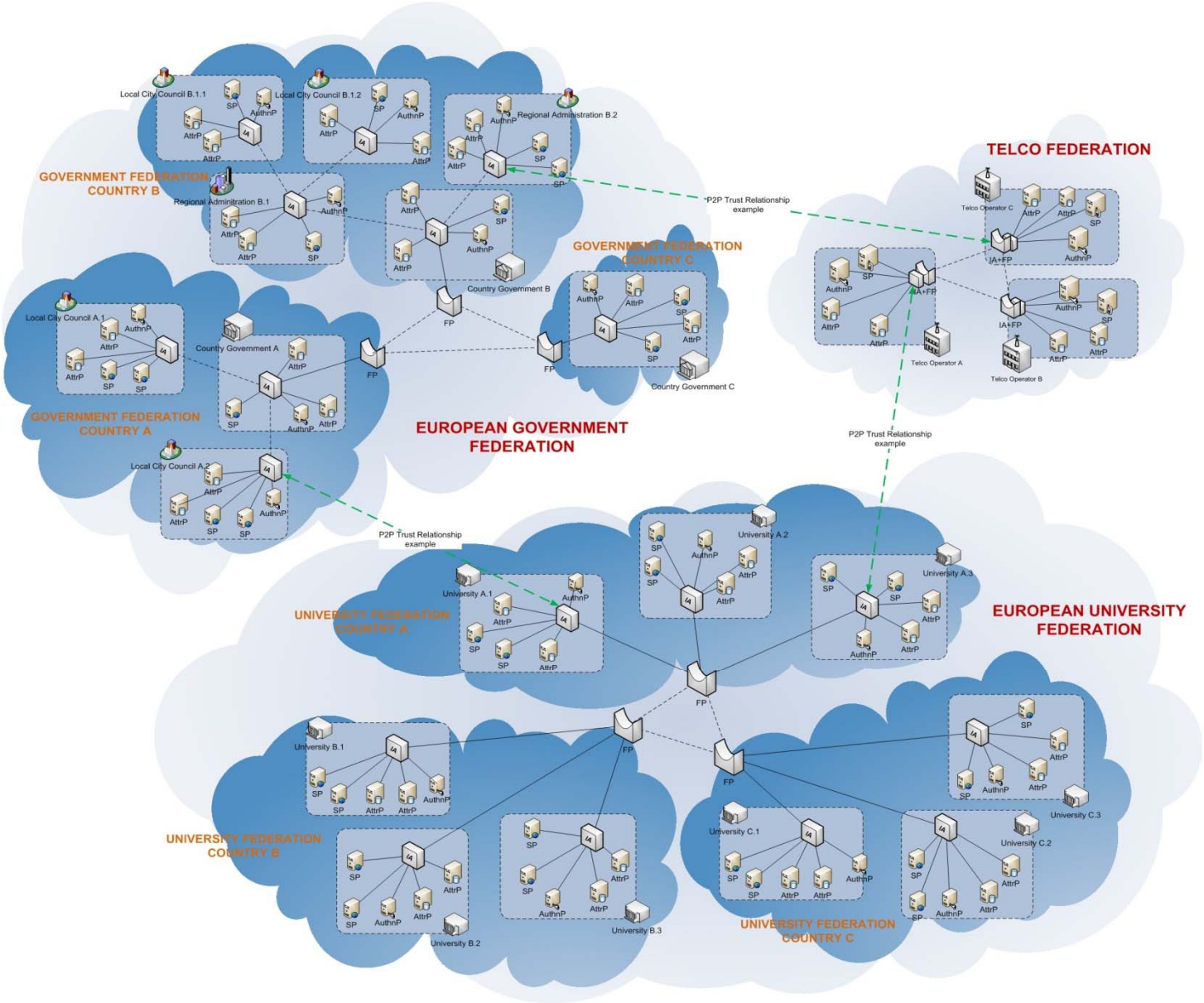


SEMIRAMIS Components - Federation Level

Several domains can be combined to a federation.



SEMIRAMIS Solution – Overall Picture



Agenda

- About SEMIRAMIS
- Architecture overview
- End-to-end privacy
- Use of pseudonyms

End-to-end privacy

- **Hop-by-hop encryption by design**
  - Attribute value encryption in AttP through SEMIRAMIS API
  - Attribute name and value aggregation in IA
  - Attribute name translation in FP (if necesary)
  - HTTPS
- **“Needs to know principle” enforced *per component***
- ***Modular architecture and policy management at each node are very important***

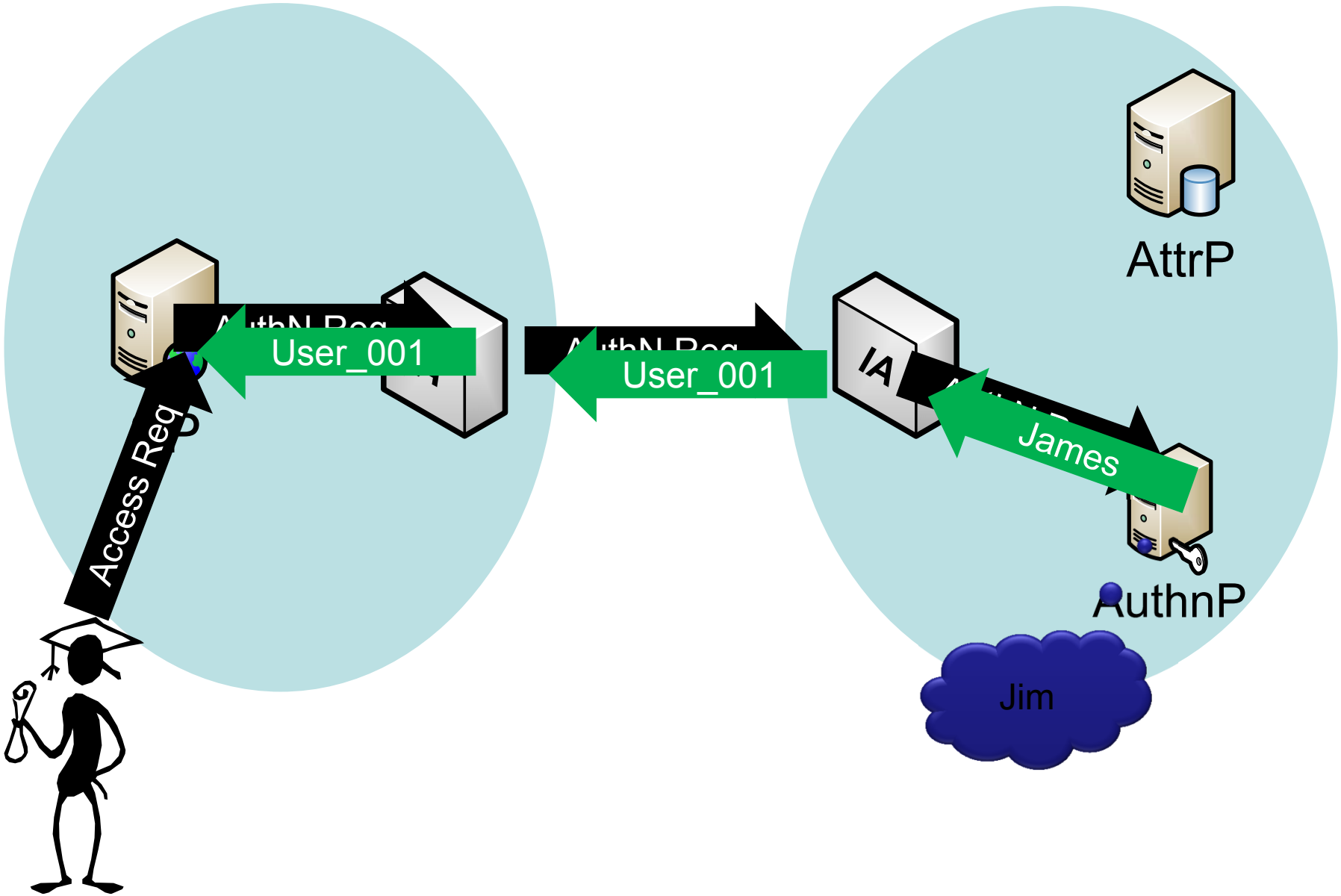
Agenda

- About SEMIRAMIS
- Architecture overview
- End-to-end privacy
- Use of pseudonyms

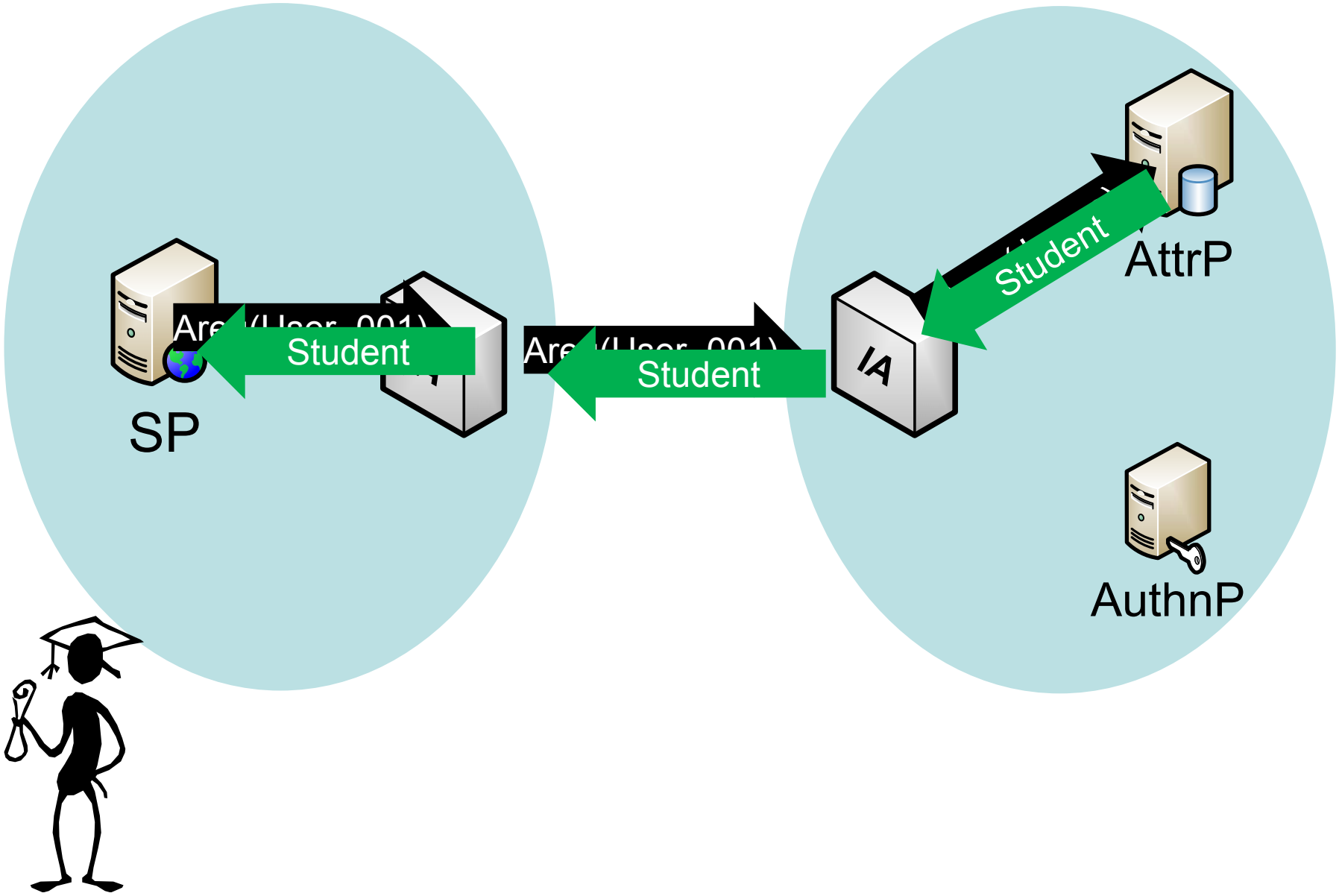
Pseudonyms

- There are three levels of pseudonymity available in the SEMIRAMIS architecture (the choice of which one should be used for a given use case should be made at design time):
  - Dynamic pseudonyms
    - These provide privacy and unlinkability. They are generated by the IA for each session.
  - Static pseudonyms
    - These provide privacy but not unlinkability: They are generated at the IA at enrolment time or on the first request for authentication, and are re-used on further requests.
  - No pseudonyms
    - In this case the IA does not modify the user identity information in any way, disclosing user information from the moment he authenticates. These do not provide privacy nor unlinkability, and are recommended for cooperative scenarios where existing protocols already specify that identity information may be freely exchanged between partners.

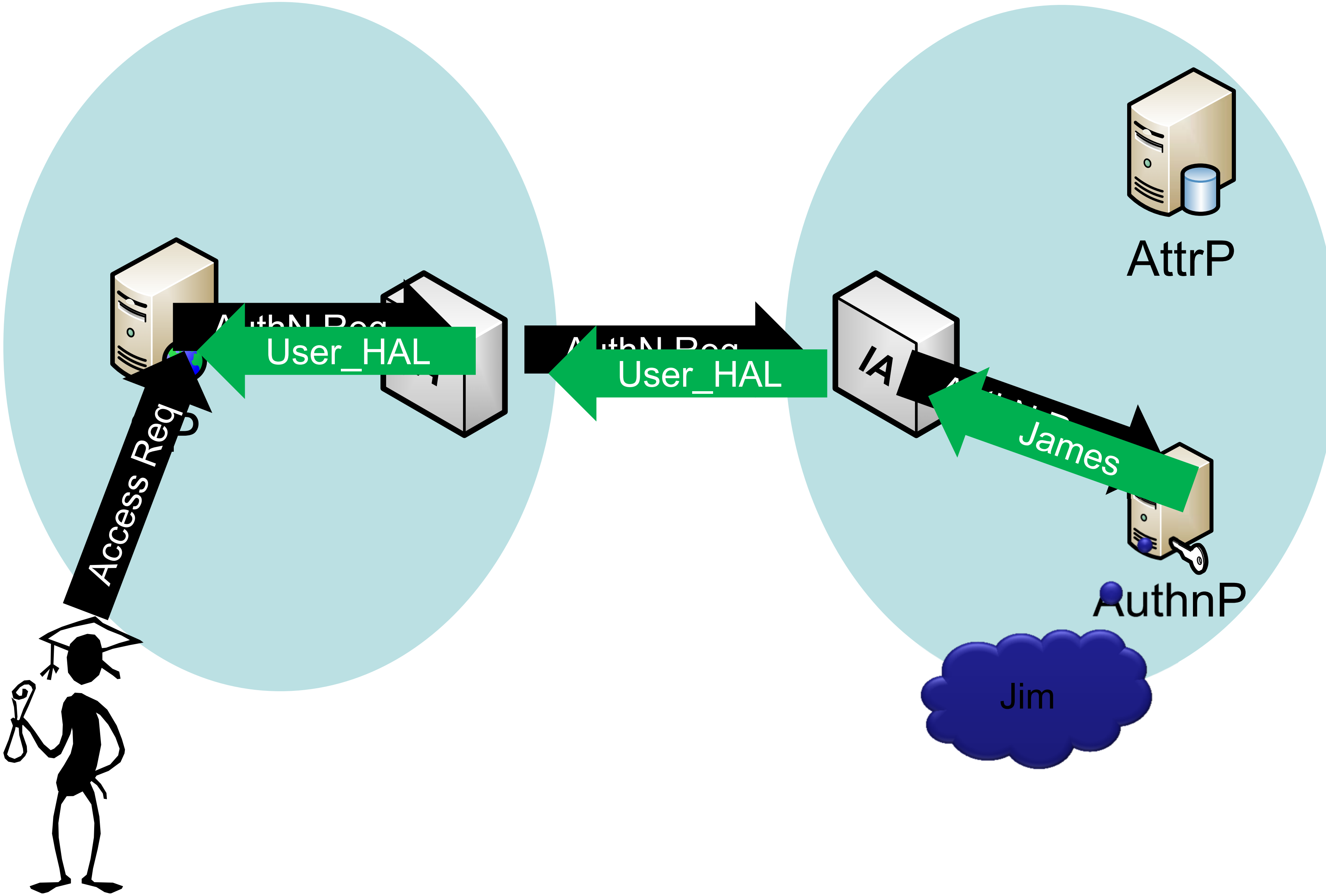
User authentication using pseudonyms



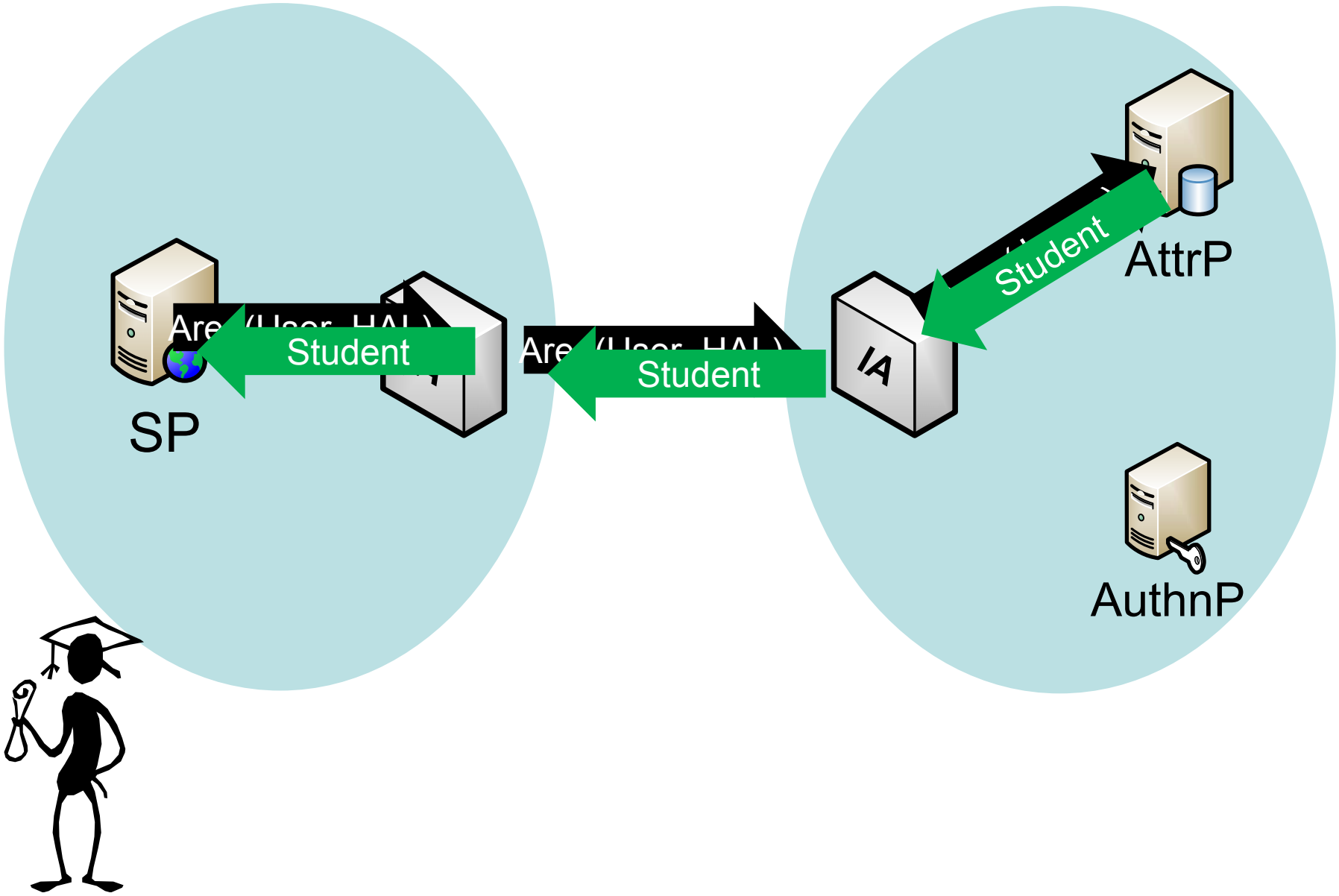
Attribute release using pseudonyms



Recurring authentication (Dynamic pseudonyms)



Attribute release after recurring authentication



Summary

- **Cross-border e-ID is important, but data (attributes) transfer is also essential (authorization)**
- **Cross-sector (multi-stakeholder) situations are not well investigated (e.g. multiple security requirements elicitation)**
- **SEMIRAMIS provides a modular architecture that can be adapted to different situations**
- **Security and privacy are part of design from the beginning, not an add-on**
- **Prototype called yourSAM (Attributes as a service) is now being offered to customers**

Thank you!

Contact:

Aljosa Pasic (ATOS): **aljosa.pasic@atosresearch.eu**

Project coordinator: Atos - (charles.bastos@atos.net – Charles Bastos)

Technical coordinator: Stuttgart Univ. (dominik.lamp@rus.uni-stuttgart.de - Dominik Lamp)