

SCHAC and Directories

tf-emc²

Victoriano Giralt

Central Computing Facility
University of Málaga

Firenze
March 28th, 2007



Outline

- 1 SCHAC
 - Awards
 - State of SCHAC
 - The future



Outline

- 1 SCHAC
 - Awards
 - State of SCHAC
 - The future
- 2 eduPersonAffiliation and controlled vocabularies



Outline

- 1 SCHAC
 - Awards
 - State of SCHAC
 - The future
- 2 eduPersonAffiliation and controlled vocabularies
- 3 Entitlement issues



Outline

- 1 SCHAC
 - Awards
 - State of SCHAC
 - The future
- 2 eduPersonAffiliation and controlled vocabularies
- 3 Entitlement issues
- 4 DNs and privacy leaks



Outline

- 1 SCHAC
 - Awards
 - State of SCHAC
 - The future
- 2 eduPersonAffiliation and controlled vocabularies
- 3 Entitlement issues
- 4 DNs and privacy leaks
- 5 URN registry status



Award for schacUserPrivateAttribute

a.k.a. irisUserPrivateAttribute

European Best Practices in Privacy Protection in the Public Sector



Award for schacUserPrivateAttribute

a.k.a. irisUserPrivateAttribute

European Best Practices in Privacy Protection in the Public Sector

RedIRIS and the University of Malaga have been awarded the first honor mention of the third edition of the award, past november, for the implementation of user controlled attribute release policies based on schacUserPrivateAttribute.



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.

Adoption of the schema is progressing



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.

Adoption of the schema is progressing, I apologize if I leave anyone out.



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.

Adoption of the schema is progressing, I apologize if I leave anyone out.

- GEANT IdP (GIdP) will use some attributes (Maurizio Molina)



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.

Adoption of the schema is progressing, I apologize if I leave anyone out.

- GEANT IdP (GIdP) will use some attributes (Maurizio Molina)
- All 11 IdP in Haka use at least schacHomeOrganization and schacHomeOrganizationType (Mikael Linden)



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.

Adoption of the schema is progressing, I apologize if I leave anyone out.

- GEANT IdP (GIdP) will use some attributes (Maurizio Molina)
- All 11 IdP in Haka use at least schacHomeOrganization and schacHomeOrganizationType (Mikael Linden)
- I swear Miro and Rok reported use of SCHAC in Croatia and Slovenia



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.

Adoption of the schema is progressing, I apologize if I leave anyone out.

- GEANT IdP (GIdP) will use some attributes (Maurizio Molina)
- All 11 IdP in Haka use at least schacHomeOrganization and schacHomeOrganizationType (Mikael Linden)
- I swear Miro and Rok reported use of SCHAC in Croatia and Slovenia
- RedIRIS uses SCHAC internally and recommends the use in Spain which has led to adoption at least at:



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.

Adoption of the schema is progressing, I apologize if I leave anyone out.

- GEANT IdP (GIdP) will use some attributes (Maurizio Molina)
- All 11 IdP in Haka use at least schacHomeOrganization and schacHomeOrganizationType (Mikael Linden)
- I swear Miro and Rok reported use of SCHAC in Croatia and Slovenia
- RedIRIS uses SCHAC internally and recommends the use in Spain which has led to adoption at least at:
 - University of Seville (production)



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.

Adoption of the schema is progressing, I apologize if I leave anyone out.

- GEANT IdP (GIdP) will use some attributes (Maurizio Molina)
- All 11 IdP in Haka use at least schacHomeOrganization and schacHomeOrganizationType (Mikael Linden)
- I swear Miro and Rok reported use of SCHAC in Croatia and Slovenia
- RedIRIS uses SCHAC internally and recommends the use in Spain which has led to adoption at least at:
 - University of Seville (production)
 - University of Basque Country(production)



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.

Adoption of the schema is progressing, I apologize if I leave anyone out.

- GEANT IdP (GIdP) will use some attributes (Maurizio Molina)
- All 11 IdP in Haka use at least schacHomeOrganization and schacHomeOrganizationType (Mikael Linden)
- I swear Miro and Rok reported use of SCHAC in Croatia and Slovenia
- RedIRIS uses SCHAC internally and recommends the use in Spain which has led to adoption at least at:
 - University of Seville (production)
 - University of Basque Country(production)
 - CICA (development)



The state of SCHAC

level of adoption

The New Year saw the final 1.3.0 version of SCHAC schema, now under the new terena.org namespace.

Adoption of the schema is progressing, I apologize if I leave anyone out.

- GEANT IdP (GIdP) will use some attributes (Maurizio Molina)
- All 11 IdP in Haka use at least schacHomeOrganization and schacHomeOrganizationType (Mikael Linden)
- I swear Miro and Rok reported use of SCHAC in Croatia and Slovenia
- RedIRIS uses SCHAC internally and recommends the use in Spain which has led to adoption at least at:
 - University of Seville (production)
 - University of Basque Country(production)
 - CICA (development)
 - University of Malaga (scheduled for production next week)



The future of SCHAC

where do we want to go

A couple of options for the development of SCHAC

- **Experimental attributes**



The future of SCHAC

where do we want to go

A couple of options for the development of SCHAC

- **Experimental attributes**

Origin

The introduction of a experimental branch stems from a need of EduGAIN that had to meet a tight deadline.



The future of SCHAC

where do we want to go

A couple of options for the development of SCHAC

- **Experimental attributes**

Experimental branch

A good thingtm

It may be useful for testing new attributes without disturbing the stabilized schema and for work in progress.



The future of SCHAC

where do we want to go

A couple of options for the development of SCHAC

- **Experimental attributes**

Pertinence of the attributes

This is an open discussion.
Should we have it now?



The future of SCHAC

where do we want to go

A couple of options for the development of SCHAC

- **Experimental attributes**

Pertinence of the attributes

This is an open discussion.
Should we have it now?

- schacProjectMembership



The future of SCHAC

where do we want to go

A couple of options for the development of SCHAC

- **Experimental attributes**

Pertinence of the attributes

This is an open discussion.
Should we have it now?

- schacProjectMembership
- schacProjectSpecificRole



The future of SCHAC

where do we want to go

A couple of options for the development of SCHAC

- Experimental attributes
- **Student information**

SCHAC document section 4.3



The future of SCHAC

where do we want to go

A couple of options for the development of SCHAC

- Experimental attributes
- **Student information**

SCHAC document section 4.3

- It is empty



The future of SCHAC

where do we want to go

A couple of options for the development of SCHAC

- Experimental attributes
- **Student information**

SCHAC document section 4.3

- It is empty
- Bologna will move lots of them around



The future of SCHAC

where do we want to go

A couple of options for the development of SCHAC

- Experimental attributes
- **Student information**

SCHAC document section 4.3

- It is empty
- Bologna will move lots of them around
- Should we start working on this?



eduPersonAffiliation and controlled vocabularies

Points of view, controlled terms, controlled meanings

We are finding that if we are going to interoperate, and use ePA in that, we need not only the same values for the attributes, but also controlled meanings.



eduPersonAffiliation and controlled vocabularies

Points of view, controlled terms, controlled meanings

We are finding that if we are going to interoperate, and use ePA in that, we need not only the same values for the attributes, but also controlled meanings.

- Europe's view

Meaning clashes

Stemming from discussions between Mikael Linden and Andrew Cormack.

fi:Employee != uk.Employee

Then there is what some spaniards think staff means :)

eduPersonAffiliation and controlled vocabularies

Points of view, controlled terms, controlled meanings

We are finding that if we are going to interoperate, and use ePA in that, we need not only the same values for the attributes, but also controlled meanings.

- Europe's view

New terms

University of Malaga has found the need for new affiliations

Someone in the UK library space has surfaced the need for library patrons



eduPersonAffiliation and controlled vocabularies

Points of view, controlled terms, controlled meanings

We are finding that if we are going to interoperate, and use ePA in that, we need not only the same values for the attributes, but also controlled meanings.

- Europe's view
- **America's view**

Work has to be done on the subject

A document should be drafted about how to work on the process.

Maybe ePA should be considered a local issue?



eduPersonAffiliation and controlled vocabularies

Points of view, controlled terms, controlled meanings

We are finding that if we are going to interoperate, and use ePA in that, we need not only the same values for the attributes, but also controlled meanings.

- Europe's view
- **America's view**

Deprecate ePA in favor of eduPersonEntitlement

During the discussion in MACE-Dir call, the issue was brought up:

May be we should recommend not using ePA for authorization, in favor of entitlements.



eduPersonAffiliation and controlled vocabularies

Points of view, controlled terms, controlled meanings

We are finding that if we are going to interoperate, and use ePA in that, we need not only the same values for the attributes, but also controlled meanings.

- Europe's view
- America's view
- **A global view?**

Time for global discussion

Should we start a discussion on what we want or need out of affiliations?

Should we try to find some common grounds for a few terms with a coarse wider meaning and move the finer grains into entitlements?

Should we move to

eduPersonScopedAffiliation?



Entitlement issues

are we overusing eduPersonEntitlement?

Our day to day use of entitlements have lead us into some questions



Entitlement issues

are we overusing eduPersonEntitlement?

Our day to day use of entitlements have lead us into some questions

- Lots of them



Entitlement issues

are we overusing eduPersonEntitlement?

Our day to day use of entitlements have lead us into some questions

- Lots of them
- Should an application see other applications entitlements?



Entitlement issues

are we overusing eduPersonEntitlement?

Our day to day use of entitlements have lead us into some questions

- Lots of them
- Should an application see other applications entitlements?
- Anyone thinking about eduPermissions or eduPermissionGroups?



DNs and privacy leaks

Use of privacy protected attributes in DN

The use of privacy controlled attributes in DN makes it impossible to hide them if policy requires, as DN are always returned to queries.



DNs and privacy leaks

Use of privacy protected attributes in DN

The use of privacy controlled attributes in DN makes it impossible to hide them if policy requires, as DN are always returned to queries.

- Attributes for DN

RFC 4514

The MUST list is short:

CN, L, ST, O, OU, C, STREET, DC, UID



DNs and privacy leaks

Use of privacy protected attributes in DNs

The use of privacy controlled attributes in DNs makes it impossible to hide them if policy requires, as DNs are always returned to queries.

- Attributes for DNs
- **Overcomplying software**

Some implementors don't like MAY part

Though there is section 5 about security and a MAY paragraph for the list of DN attributes, some implementors decide just to stick to the MUST.



DNs and privacy leaks

Use of privacy protected attributes in DNs

The use of privacy controlled attributes in DNs makes it impossible to hide them if policy requires, as DNs are always returned to queries.

- Attributes for DNs
- Overcomplying software
- Options?

What has happened to DNC?

Anyone knows if discussions about DNC got anywhere?
Should we work on that?



URN

what have we been doing this months

Work has been progressing, though not as fast as I would like.



URN

what have we been doing this months

Work has been progressing, though not as fast as I would like. That means, we have room for steering, which means mainly questions for you.



URN

what have we been doing this months

Work has been progressing, though not as fast as I would like. That means, we have room for steering, which means mainly questions for you.

- We have a project in RedIRIS GForge:
<https://forja.rediris.es/projects/urnreg/>



URN

what have we been doing this months

Work has been progressing, though not as fast as I would like. That means, we have room for steering, which means mainly questions for you.

- We have a project in RedIRIS GForge:
<https://forja.rediris.es/projects/urnreg/>
- REST vs SOAP



URN

what have we been doing this months

Work has been progressing, though not as fast as I would like. That means, we have room for steering, which means mainly questions for you.

- We have a project in RedIRIS GForge:
<https://forja.rediris.es/projects/urnreg/>
- REST vs SOAP
- Data definitions



Summary

Summary should come out our discussions on the matter.

