



# 7<sup>th</sup> FIM<sub>4</sub>R meeting

23-24 April 2014

ESRIN

Frascati



# Meeting agenda

Agenda page online with material:

<https://indico.cern.ch/event/301888/>

A written summary will be produced of this event

Dinner pick-up at 19:30

**FIM4R**

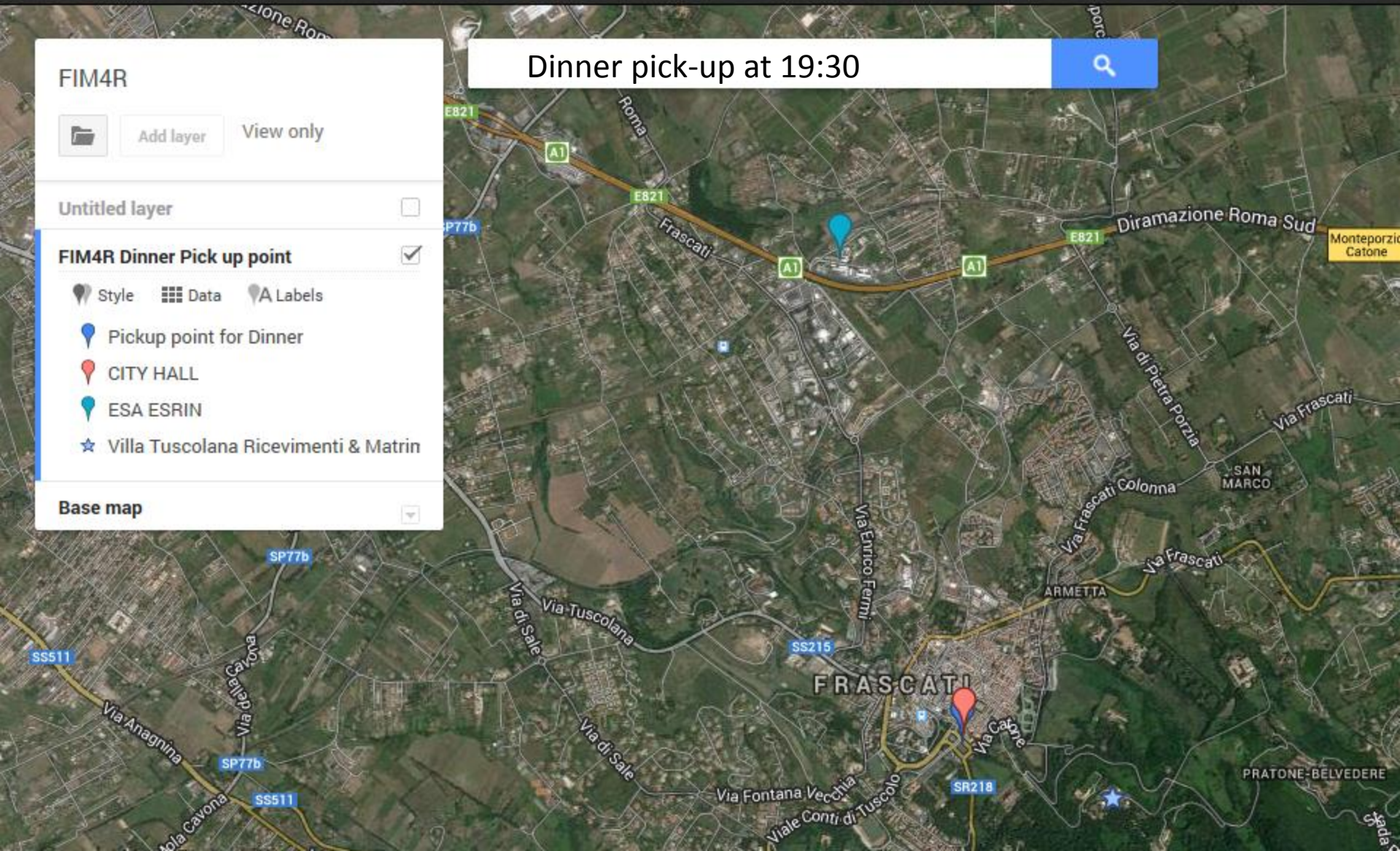
Add layer View only

Untitled layer

**FIM4R Dinner Pick up point**

- Style Data Labels
- Pickup point for Dinner
- CITY HALL
- ESA ESRIN
- Villa Tuscolana Ricevimenti & Matrin

Base map





# This afternoon

Objective: *User Communities view of the progress made since the first publication of the Federated Identity Management for Research Collaborations paper and priorities for the future*

Roundtable introductions

- Summary of Terena AAI workshop (Licia Florio)
- Operational Security (Romain Wartel)

Coffee

- Working with service providers in the future
- H2020 – how do we work together?

End of the session: 17:30

ESA shuttles to Frascati 17:30 & 18:15 (outside main gate)

# Federated Identity Management for Research Collaborations

Paper Type: Research paper

Date of this version: 28 August 2013

**Abs**

Federated  
subscri  
group  
For ex  
resour

A num  
deluge

organisational and national boundaries.

- **Requirements from the research communities**
- **Status of the activities & use cases**
- **Common vision across these communities**
- **Key stages of a roadmap**
- **Set of recommendations**

lets  
the  
ers.  
n of  
of a  
ross

Driven by these needs, representatives from a variety of research communities, including photon/neutron facilities, social science & humanities, high-energy physics, atmospheric science, bioinformatics and fusion energy, have come together to discuss how to address these issues with the objective to define a common policy and trust framework for Identity Management based on existing structures, federations and technologies.

This paper will describe the needs of the research communities, the status of the activities in the FIM domain and highlight specific use cases. The common vision for FIM across these communities will be presented as well the key stages of the roadmap and a set of recommendations intended to ensure its implementation.

**Keywords**

federated identity management, security, authentication, authorization, collaboration, community

Authors: Daan Broeder, Bob Jones, David Kelsey, Philip Kershaw, Stefan Lüders, Andrew Lyall, Tommi Nyrönen, Romain Wartel, Heinz J Weyer





# The FIM<sub>4</sub>R Vision

**A common policy and trust framework for Identity Management based on existing structures and federations either presently in use by or available to the communities.**

**This framework must provide researchers with unique electronic identities authenticated in multiple administrative domains and across national boundaries that can be used together with community defined attributes to authorize access to digital resources.**



# Prioritisation of FIM<sub>4</sub>R requirements

- **User friendliness (high)**
  - Support for citizen scientists and researchers without formal association to research labs or univ
- **Browser & non-browser federated access (high)**
- **Bridging communities (medium)**
  - Bridging is a central issue with an efficient mapping of the respective attributes
- **Multiple technologies with translators including dynamic issue of credentials (medium)**
- **Implementations based on open stds and sustainable with compatible licenses (high)**
- **Different Levels of Assurance with provenance (high)**
  - Credentials need to include the provenance of the level under which it was issued
- **Authorisation under community and/or facility control (high)**
- **Well defined semantically harmonised attributes (medium)**
- **Flexible and scalable IdP attribute release policy (medium)**
  - Bi-lateral negotiations between all SPs and all IdPs is not a scalable solution
- **Attributes must be able to cross national borders (high)**
  - Data protection considerations must allow this to happen.
- **Attribute aggregation for authorisation (medium)**
  - Attributes need to be aggregated from different sources of authority including federated IdPs and community-based attribute authorities.
- **Privacy and data protection addressed with community-wide individual ids (medium)**

# Technologies being piloted by resource communities

	Technology	Inter-federation	Status	Plans
ELIXIR	SAML2	Joined to the HAKA federation.	Development	Join eduGAIN and Kalmar union.
ESA	Shibboleth		Production	Join NASA and EUMETSAT
WLCG	Web based and non-web based. Pilot project on non-web based. SAML2.		CLI solution achieved but looking into alternatives.	Refocus on web-based use case.
DARIAH	Shibboleth		Development	Implement DARIAH-EU
SWITCH	Shibboleth	Open to inter-federation with eduGAIN.	Production (for the majority of Swiss Universities)	Moonshot and Interfederation with eduGAIN
CLARIN	Shibboleth		Implementation	Interconnection through Service Provider Federation (SPF)
Umbrella	Shibboleth	Bridging concept being developed.	Implementation	Affiliation Database, Sync with other programs iCAT, Moonshot. Bridging. Implementation up to Sept. 2013.
WeNMR	Drupal based VON NMR VRC, Shibboleth authN, phpCAS authN, robot certificates.	Flexibility to connect to a wide set of federations (from Drupal).	Production	
SyBIT	Azure	Any federation could be easily integrated.	Microsoft product.	Self-federation model.





# Research Infrastructures need a **service**

- **Risk Analysis** - *implications of having a malicious SP in a federation*
- **Traceability** - *identifying the cause of any security incident*
- **Security Incident Response** – *including all IdPs and SPs*
- **Transparency** - *essential to gain the trust of the users and service providers*
- **Reliability and Resilience** - *of the framework services*
- **Smooth Transition** - *of the existing production systems to a federated identity management model*
- **Easy integration with local SP environment** - *SPs are likely to want to support multiple means of authentication*
- **Specific requirements** - *from some communities*