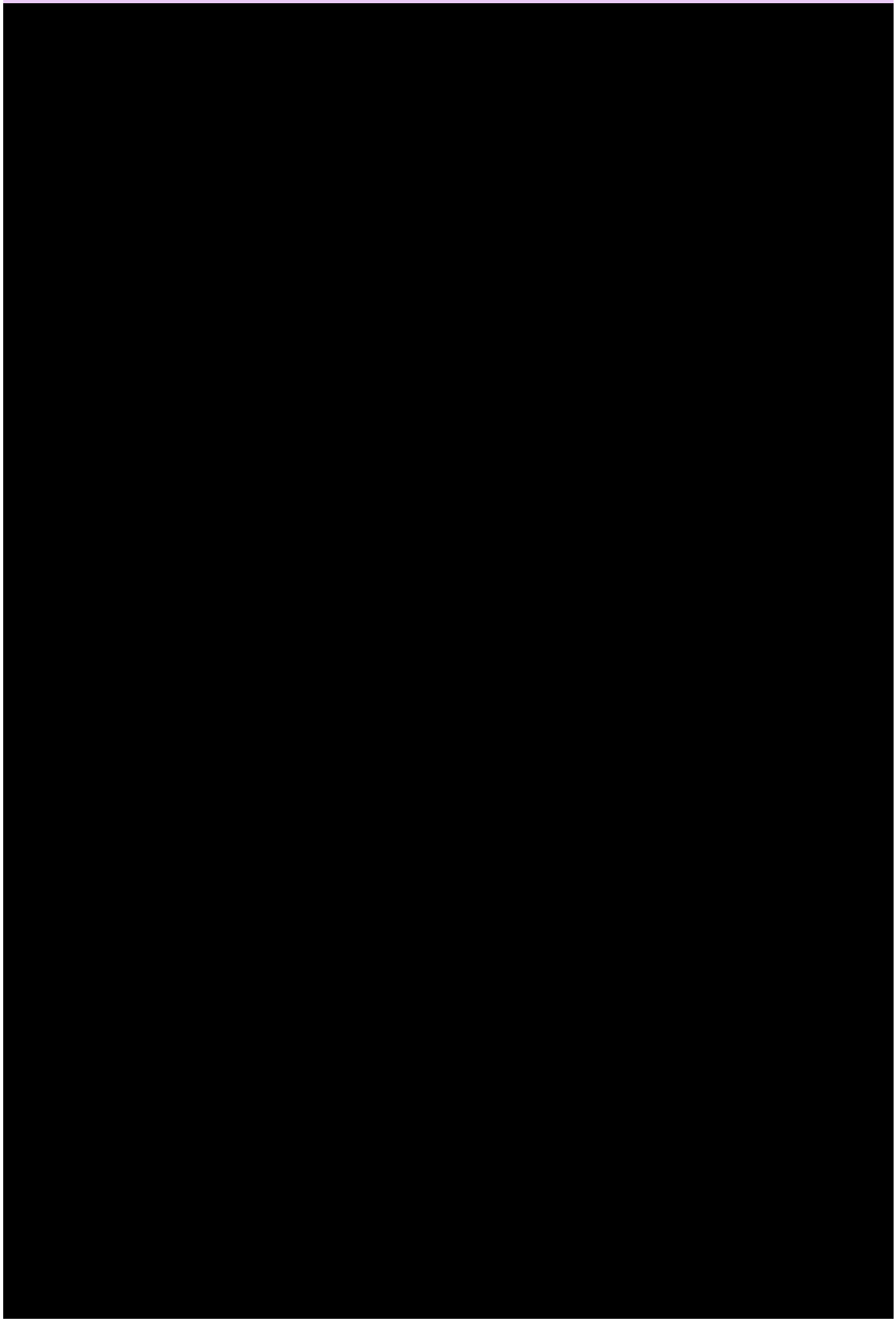

1 Federated Identity Management on scientific collaborations

The objetives of my new project are to develop and deploy a pan-European system for unique identification (Authentication and authorisation infrastructure: AAI) of users at the infrastructures of the participating RIs EuroFEL (PSI), ESRF, ESS, FAIR (GSI), ILL, and XFEL for the management of local and remote access to facilities, experiments, data, and IT resources.

Identity Management System is the set of tools needed to manage the identity of people. (*Wikipedia source*)An IdM (Identity Management) system comprises:

1. Establishment of the identity.
2. Describes the identity.
3. Follows identity activity.
4. Destroys the identity.

When we talk about **Federated IdM** the we are providing a mean for partner services to agree on and establish a common, shared name identifier to refer to the user in order to share information about the user across the organizational boundaries.

1.1 Motivation

The main goal of look into Federated access for scientific communities is because those communitites are facing similar challenges. The user community is growing. The less barriers those users face, the better. Also, federated identity management is good for security because reduces the amount of accounts needed for a user (identity providers have the attention of attackers). There are a set of common needs from those communities (gathered in the 1st workshop on Federated Identity Management in Scientific Collaborations):

1. Need for single-sign on access.
2. Ease of use for part-time users.
3. Controlling access to the resources.
4. Support for homeless researchers.
5. Interoperability accross national boundaries.
6. Trust is needed with accreditation. IGTF is already in use by many of the communities.
7. Traceability.

8. Enable federated access from grids of High Performance Computing, as well as High Troughput Computing and new Distributed computing resources, such as Clouds, Supercomputing networks and Desktops grids.

1.2 State-of-the-art technologies and tools

As a first step I will research the state-of-the-art technologies and tools currently used or being adopted by other scientific collaborations. I attended the 1st workshop on Federated Identity Management in Scientific Collaborations and the 2nd workshop on Federated Identity Management in Scientific Collaborations, where the main user-requirements, existing technologies and vision on this subject were presented.

Organisation	#users	Main concern	Tool used
PSI	~ 10000	Very big datasets, that want to access remotely.Very short lived users. Homeless users.	Umbrella (shibboleth + SAML)
CLARIN	hundreds	Single domain with identity managed by home institute. Many diverse and distributed data sets with complex relations in between them.	eduGAIN (Shibboleth + SAML)
WLCG	~5900	IGFT is the approach to federated IdM. This solution does not scale. In the Grid it is difficult to identify the original source of compromise. x509 needs to be supported (security token service)	x509
ESGF (earth system grid fed.)	~5000	Already many technologies existing.Single sign on with OpenID and MyProxy.Attribute propagation with SAML and OpenID. Authorisation with SAML.	openID + SAML
OSG (open science grid)		They want to integrate together InCommon and IGTF	SAML + Shibboleth + x509

1.2.1 SAML

SAML enables web-based authentication and authorization scenarios including single sign-on. Following a short description of SAML 2.0 from SAML technical overview. The three main goals of this technology are:

1. Single sign-on. SAML solves the supported multi-domain SSO (MDSSO) problem by providing a standard vendor-independent grammar and protocol for transferring information about a user from one web server to another independent of the server DNS domains
2. Federated identity management. The user is said to have a federated identity when partners have established an agreement on how to refer to the user.
3. Web services and other industry standards. SAML allows for its security assertion format to be used outside of a native SAML-based protocol context.

2 Chef

Machines where I have chef server installed: lxgrid5, depc318.

This web page has been written using markdown language, and converting it to HTML with Conversio