

SPECIFICATION FOR THE FENIX FEDERATED AUTHENTICATION AND AUTHORIZATION INFRASTRUCTURE



Implementation of the Fenix Authentication and Authorization Infrastructure (AAI)

Table of contents

1. Introduction	3
2. Glossary	3
3. ICEI Project overview	4
3.1 The Fenix Authentication and Authorization Infrastructure (AAI).....	4
3.1.1 High-level AAI infrastructure design	4
3.1.2 Fenix AAI Implementation strategy	6
4. Goal of this procurement	6
5. Technical specifications	6
5.1 Categories of requirements	6
5.2 The Fenix Central Proxy IdP	7
6. Maintenance and support.....	9
7. SLA of maintenance and support services.....	10
7.1 Help desk and troubleshooting.....	10
7.1.1 Inactive users	11
8. Relations with the supplier	11
9. Installation plan.....	11
9.1 Validation	11
10. Data Protection	11

1. Introduction

The purpose of this document is to describe how the Authentication and Authorization Infrastructure (AAI) of the Fenix e-Infrastructure is organized and how it will be implemented through the support of an external service provider. The document introduces the ICEI project, the main components of the Fenix infrastructure, and the rationale behind our technical choices.

2. Glossary

Term	Description
Backbone	Site-wide Ethernet network (40GE or 100GE)
BGP	Border Gateway Protocol
Cineca	Interuniversity Consortium
DDR	Double Data Rate
DIMM	Dual In-line Memory Module
DWDP	Device/drive writes per day
ETP	European Technology Platform
EUDAT	European Collaborative Data Infrastructure
GPGPU	General-Purpose computing on Graphics Processing Units. Graphic processing unit usable for computation
HA	High-Availability. Mechanism to ensure service availability in case one of a component failure
HBP	Human Brain Project. H2020 FET Flagship Project funded by the European Union
HPC	High-Performance Computing
HPSS	High Performance Storage System, developed by IBM. Hierarchical Storage Manager that can store data on multiple levels of storage (disks, tapes ...)
ICEI	Interactive Computing e-Infrastructure
IOPs	Interactive Computing e-Infrastructure
NMV	Non-volatile memory
OpenStack	Open-source software platform for cloud computing
PCIe	Peripheral Component Interconnect Express
PDU	Power Distribution Unit
POSIX	Portable Operating System Interface for Unix
Puppet	Tool for configuration management
PRACE	Partnership for Advanced Computing in Europe
RAID	Redundant Array Of Inexpensive Disks. Mechanism to prevent from disk failures by storing redundant information on additional disks (mirror, parity...)
Robinhood	Open-source policy engine to monitor file-system contents and apply automatic actions on file-system entries according to admin-defined policies (migration, purge...)
SDRAM	Synchronous Dynamic Random Access Memory

SPOF	Single Point Of Failure. Part of a system that, in case of failure, prevent the whole system from working
SPOM	Single Point Of Management. Server(s) that provide centralized monitoring and administration services
SR-IOV	Single-root input/output virtualization
SWIFT	Object storage in the OpenStack platform
UPS	Uninterruptible Power Supply
VM	Virtual machine

3. ICEI Project overview

ICEI¹ (Interactive Computing e-Infrastructure) is a collaboration project partially funded by the European Commission involving the leading European HPC Centres such as BSC (Spain), CEA (France), CINECA (Italy), CSCS (Switzerland), and FZJ/JSC (Germany). The project will deliver a set of e-infrastructure services that are federated to form the Fenix infrastructure. The distinguishing characteristic of this e-infrastructure is that data repositories and scalable supercomputing systems will be in close proximity and well integrated. The European Human Brain Project will be the initial prime user of this research infrastructure. It will take care of developing the community-specific services on top of the Fenix infrastructure services. Part of the resources within the ICEI infrastructure will be provided to European researches at large through PRACE. In the future other communities are expected to leverage the Fenix e-infrastructure.

3.1 The Fenix Authentication and Authorization Infrastructure (AAI)

In order to provide access to the **Fenix infrastructure services**, the federation needs to rely on a robust and reliable Authentication and Authorization Infrastructure (AAI), a trustworthy environment through which users can be authenticated to access resources securely and as **seamlessly** as possible. For seamless access it is meant the capability for an user, registered on a “trusted” Identity Provider² (IdP) and granted to consume a certain amount of resources, to access resources using his/her credentials (i.e. username/password, X.509, etc..) without going through any further registration process or multiple authentication steps.

The federation should be able to leverage on existing IdPs currently managing access to ICEI partners (BSC, CEA, CINECA, CSCS, JSC) and be able to grow if other institutions demand to join.

3.1.1 High-level AAI infrastructure design

The Fenix AAI is conceived as the interoperation of two distinct services, a Central Proxy IdP that is responsible to proxy authentication requests among federated IdPs, and an Attributes Provider, named FURMS (FENIX User and Management Service), managing users authorization records such as budget allocation, groups and roles membership.

The two services have been designed to deliver the following functionalities respectively:

- **Fenix Central Proxy IdP (Service 1)**
 - Proxy of users authentication requests
 - Users identification and authentication (homeless users)
 - Validation of users profile attributes
 - Policy registry and management of principles of engagement

¹ The ICEI project has received funding from the European Union Horizon 2020 research and innovation programme under the grant agreement No 800858

² Any IdP part of the federation releasing common attributes for the user

- **FURMS (Service 2)**
 - Groups/projects membership management
 - SSH public keys management
 - Managing site specific Usage Agreements
 - Access statistics and accounting

The reason behind the separation of functionalities between two services is twofold:

- To keep the Central Proxy IdP as lean as possible in order to provide high operation performance;
- To improve infrastructure security by decoupling highly critical functions from less critical ones.

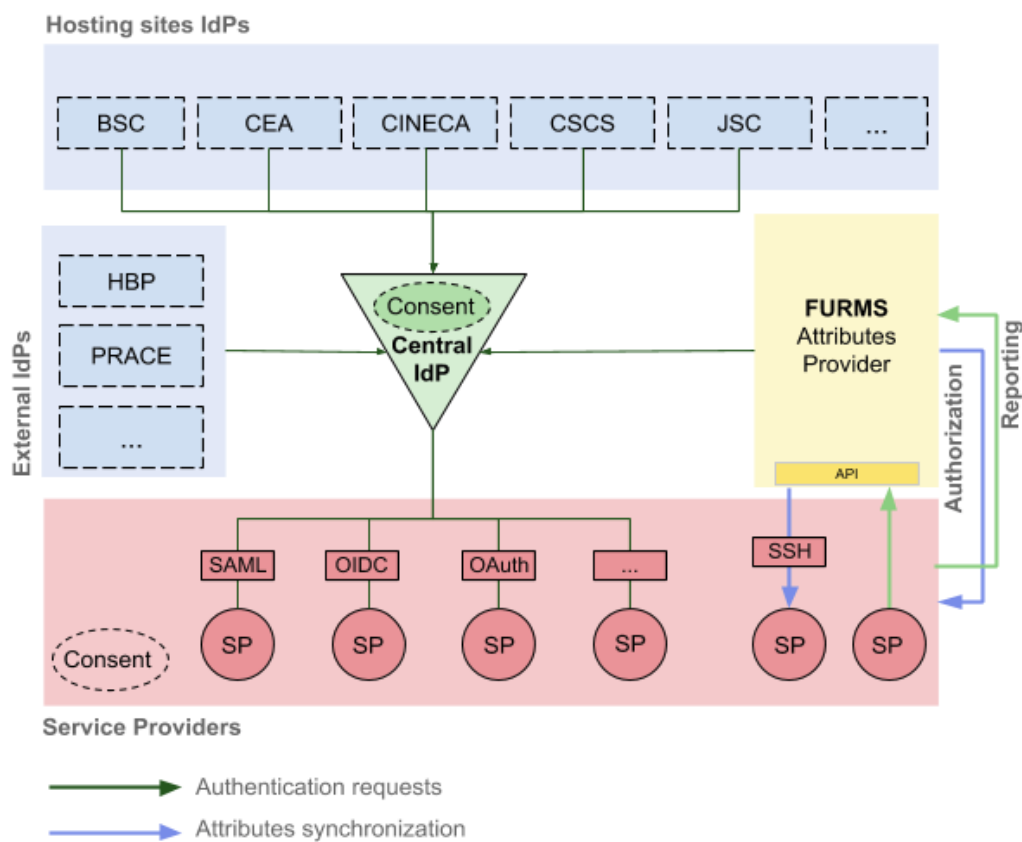
This document provides details on the first service only.

For every user requesting to access the Fenix infrastructure, a new profile will be created on the Fenix Central Proxy IdP including a minimum set of attributes, a permanent and opaque³ **Fenix identifier** and a **Fenix username**.

The creation of a Fenix profile for each user is fundamental for the following reasons:

- to get him/her accept the general Fenix access policy;
- to trace his/her actions within the federation uniquely;
- to associate his/her identity to a project/budget – via FURMS - in order to consume resources.

The **Fenix identifier** and the **Fenix username** will also serve to identify users while accessing Fenix services.



Fenix AAI High-level architecture

³ <https://indieweb.org/opaque>

3.1.2 Fenix AAI Implementation strategy

The overall Fenix AAI architecture is the result of a co-design effort between CINECA, as coordinator of the AAI activity within the ICEI project, and project members (BSC, CEA, CINECA, CSCS, JSC). However, each site is responsible for providing all the necessary information in order to federate local IdPs and SPs (Service Providers) with the Central Proxy.

4. Goal of this procurement

The procurement will serve to purchase:

- The provisioning of a scalable **Central Proxy IdP service** able:
 - to federate Fenix partners IdP and respective SPs via open common federation protocols such as SAML (Security Assertion Markup Language), OAuth, OpenID, Security Tokens (Simple Web Tokens, JSON Web Tokens, and SAML assertions), Web Service Specifications;
 - to proxy authentication requests, up to 200 concurrent requests per second, and provide access to Fenix services and resources within;
 - to be reached through the public network;
 - to manage thousands of users profile.

Hardware resources: the supplier should provide hardware resources and configuration setup in order to support the deployment of the Fenix Central Proxy IdP and to satisfy service levels expectation.

Development environment, including demo software components to mimic basic functionalities. This includes:

- Demo Central Proxy IdP instance
- Dummy SAML SP for testing
- Dummy User Resource Management system for testing (will be replaced by FURMS). This is not mandatory, but would be better if it is provided.
- Some web page link where user profile attributes can be read by the administrators of the SPs

5. Technical specifications

5.1 Categories of requirements

The following sections detail the requirements, target capabilities demand for the Central Proxy IdP service.

The items are numbered to enable the proposals to refer to specific items. Where applicable, a coarse time line target (categories “early”, “midway”, “late”) is specified to provide the candidates a guideline concerning the public procurers temporal prioritization of the requirements. The details are subject to the negotiations.

Seq. No.	Description	Category
----------	-------------	----------

1	Mandatory Requirements are considered essential for the procured system and must be fulfilled by all Final Proposals. Mandatory Requirements will be assessed for each Proposal submitted. Final Proposals which will not be compliant with all Mandatory Requirements will be rejected.	MRQ
2	Target Capabilities are desirable features and desirable performance levels for the procured system. In contrast to Mandatory Requirements, failure to provide Target Capabilities will not lead to the rejection of the Final Proposals provided by the Tenderer. Proposals that provide the Target Capabilities will receive a higher score. Target Capabilities are prioritized. Level-one priority Target Capabilities (TC-1) are considered of higher importance than level-two Target Capabilities (TC-2)..	TC-1 TC-2

Requirements, target capabilities and requested documentation for the scope.

5.2 The Fenix Central Proxy IdP

Table below includes all the base requirements that the Fenix Central Proxy IdP should comply with. Besides the adoption of open identity federation protocols as reported above, the supplier is free to decide which technology to use to implement the service.

Seq. No.	Requirement description (functional)	Category
1	The Central Proxy IdP should provide an Identity and access management solution aimed at modern applications and services. The Central IdP should be capable of federating with external Identity Providers supporting open identify federation protocols.	MRQ
2	Single-Sign On: once users are authenticated through the Central IdP they do not have to login again to access a different application or domain. The Proxy works in order to rely on the SSO capabilities of the home IdPs. This means that every authentication request is proxied to a specific home IdP “transparently”.	MRQ
3	The Central IdP should not provide also Single-Sign Out in principle. This can be supported at the Proxy level, but we cannot avoid users still having active sessions on the local SPs or home IdPs. Anyway the Proxy could be configured in order to exploit proper remote APIs on sites (if these are provided) in order to delete local sessions.	MRQ
4	It should be accessible by all Fenix sites in the federation.	MRQ
5	It should support the following classes of IdPs: Fenix hosting sites (BSC, CEA, CINECA, CSCS, JSC), Primary research communities (HBP), eduGAIN /Other research communities, ORCID	MRQ
6	Should export a minimum set of attributes for each user to the sites SPs (Name, Family Name, Email, Institution(s) or affiliation(s), Fenix identifier, Fenix username)	MRQ
7	The IdP should be capable to accept SAML attributes and OIDC claims from all sites and harmonise them based on the FENIX AAI requirements	MRQ
8	Should manage the Fenix username and Fenix identifier for each Fenix user. The Fenix identifier could be calculated using pairwise identifiers (e.g. “sub” claim and salt), concatenated and hashed using i.e. SHA-256	MRQ
9	Should provide user profile management , i.e. check attributes validity on a regular basis	MRQ
10	Support federation with local site IdPs and SPs through standard protocols: SAML2, OIDC	MRQ

11	Should provide Token Translation Service mechanism, at least for SAML2 and OIDC Tokens	MRQ
12	Should provide mapping between OIDC and SAML2 attributes	MRQ
13	Should present Fenix terms and conditions to be accepted by users in order to be profiled on the Fenix Central Proxy IdP. The terms and conditions will be defined by Fenix and provided to GÉANT	MRQ
14	Should keep trace of signed policy agreements for users	MRQ
15	Should provide a base Account Linking mechanism. Details will be defined between Fenix and the Supplier	MRQ
16	Multiple Level of Assurance (LoA) should be supported for users. Details will be defined between Fenix and the Supplier	MRQ
17	OIDC token introspection and validation for non-web services (e.g. OpenStack SWIFT ⁴ or UNICORE ⁵): https://connect2id.com/blog/how-to-validate-an-openid-connect-id-token This feature may include deep-delegation , this is something that may require additional effort to the supplier for the implementation.	TC-1
18	Provide interfaces for both web and application level authentication	MRQ
19	Provide a REST API for basic operations.	MRQ
20	Could be eventually integrated with external data sources (e.g. LDAP or MySQL)	MRQ
21	Should be eventually integrated also with external services, e.g. FURMS, The proxy should be capable to query a generic remote service, exploiting provided remote APIs	MRQ
22	Fenix AAI should be capable to validate x509 certificates. This capability should not be provided directly by the Central IdP, but could be provided i.e. by a local site IdP supporting x509 authentication and connected to the Central IdP. The Central IdP will be capable however to support such scenario	MRQ
23	Should manage inactive users . Users that are considered inactive for one year should have the account blocked and Fenix sites should be notified	MRQ
	Requirement description (non-functional)	Category
24	Should provide High Availability (HA) and Scalability , managing an order of thousands of users (Fenix sites manage 3-4000 users each). The Proxy should be able to scale up as requests increase over the time, up to 200 parallel requests per second as a peak. Furthermore, the proxy must be to support at least 10.000 registered users.	MRQ
25	Should comply with basic security requirements : HTTPS + host certificate enabled, Firewall policies properly configured, Headers security defences (e.g. X-Frame-Options: SAMEORIGIN, Content-Security-Policy, X-Content-Type-Options, X-Robots-Tag, X-XSS-Protection). Brute Force Detection could be supported on local sites, since the Proxy does not know if the user authentication succeeded or failed (maybe it could but indirectly)	MRQ
26	The IdP should provide an administrator console to centrally manage user account and profiles.	MRQ
27	The IdP technology should be supported in a long term view	MRQ

⁴ <https://docs.openstack.org/swift/latest/>

⁵ <https://www.unicore.eu/>

5.2.1 Security features

Seq. No.	Description	Category
28	It must be possible to propagate the suspension of accounts to the local sites in a timely manner. Details are subject to negotiation, as this involves site local components.	MRQ
29	All communication is secured against unwanted or malicious interception and manipulation.	MRQ
30	All communication of the web-base user interface only takes place with authenticated parties, with the sole exception of accessing the login page and any static content required for the general function of the interface.	MRQ
31	Communication among system components, i.e. the central FURMS instance, central proxy IdP, as well as the site local agents, must be authenticated.	MRQ
32	Authorization for actions within the Central Proxy IdP must be based on attribute based access control (ABAC) with attributes scoped to the resources under consideration.	MRQ
33	An audit trail of relevant actions must be available. This includes, but is not limited to: <ul style="list-style-type: none">• login and logout of users,• all management actions at all levels.	MRQ

5.2.2 Documentation and training

Seq. No.	Description	Category
34	The proposal includes training for the system administrators and relevant staff regarding the proxy operation. The training will provide an introduction to the web interface and administration panel. Scope and duration of the training should be appropriate for the complexity of the solution. Training may be performed: <ul style="list-style-type: none">• online,• preferred: training course at one of the sites. Details are subject to negotiation.	MRQ

6. Maintenance and support

CINECA requires the Central Proxy IdP to be operational for at least 5 (five) years. The supplier must ensure the features of the maintenance and support service listed below for the same duration.

- Release of software updates and bug fixing for the Central Proxy IdP, the term “update” also refers to new versions ("releases") of the software.
- Assistance with configuration and tuning of the Fenix Central Proxy IdP and, in general, for everything concerns the technology adopted for the Central Proxy IdP.
- Support for malfunctioning of hardware or software components supplied, as well as fault opening procedures.
- All maintenance and service interventions must be properly documented.
- The supplier or its agent is required to provide the necessary technical assistance, strictly respecting the conditions and the intervention times defined in the contract.

- The supplier is responsible of the professionalism of the technicians in charge.

The intervention must ensure complete restoration of full operation, as transparently as possible towards the Fenix users and the administrators of sites IdP/SPs. Ordinary maintenance includes all of the hardware and software, with the obligation to replace any affected part without exception and at no further charge for the Fenix consortium.

7. SLA of maintenance and support services

The supplier must ensure the following service levels:

- Technical support for the AAI infrastructure:
 - Support and maintenance is provided for normal working hours (5x8 hours per week excluding weekends and public holidays in Italy). Selected additional days may be excluded from the support and maintenance coverage to account for foreign holidays.
- **Response Time in case of service failure:** 1h max within working hours.
- **Resolution time:** this should be split both for CRITICAL and NOT CRITICAL functionalities
 - **CRITICAL** (4h working hours, half a day)
 - The Central Proxy IdP is not responding
 - The user authentication fails due to a failure or a bug
 - A security vulnerability has been found
 - **NOT CRITICAL** (24h working hours, 3 days more or less)
 - The site notification service (e.g. for users who fail to renew their registration for more than a year) does not work
 - A software update (not critical) is needed

7.1 Help desk and troubleshooting

During the validity period of maintenance and support services, the supplier help desk service should be accessible via email. The help desk is deputed to the following activities:

- support for troubleshooting hardware or software components of the Fenix Central Proxy IdP;
- provide assistance for the configuration, tuning and best use of the Fenix Central Proxy IdP;
- coordinate the delivery of software updates for the Central Proxy IdP with sites, in case this is requested by the supplier;
- answer promptly for the request of further improvements (i.e. requests for federating novel IdPs or sites to the Fenix Central IdP);
- coordinate the assignment of on-site technician(s) to fix critical issues as hardware failures, software bugs and so on, within a maximum period of 1 working hour;
- coordinate the assignment of on-site technician(s) to fix non critical issues (i.e. software updates, non-critical bugs and so on) within a maximum period of 3 working hours.

Furthermore, the supplier must ensure the minimum service levels described below regardless the service is delivered directly or provided through the collaboration of a subcontractor.

- Email receive period: weekdays from 09:00 to 18:00
- Response time: within 1h for 90% of the requests

The supplier must ensure at least the diagnosis of any malfunction reported by Fenix sites or users within four (4) working hours from receiving the call. In case this is needed all Fenix sites must be contacted to start the problem determination phase.

7.1.1 Inactive users

For security reasons, users inactive for one year should have the account blocked. For this reason, the Fenix Central Proxy IdP should lock the Fenix account and inform all sites.

8. Relations with the supplier

Upon awarding the contract and for the conclusion of the contract the supplier, in agreement with Fenix and CINECA, must nominate a representative to manage all relations with Fenix (i.e. through a specific mailing list). The representative is the point of contact for any issues that Fenix considers unresolved within the normal relationship with the supplier.

9. Installation plan

The supplier is responsible for the installation, operation, configuration and tuning of the Fenix Central Proxy IdP, including hardware and software provisioning.

9.1 Validation

The installation is considered completed once the supplier has installed and configure all the elements needed to implement the basic functionalities described in this document. Moreover all the functional and workload tests relating to the mandatory requirements (MRQ) of the Fenix Central IdP (authentication, user profiling, profile validation, account linking and so on) should have been successfully performed. Not mandatory requirements can be eventually implemented further, in collaboration with CINECA.

10. Data Protection

The GDPR requires to implement controls and processes for protecting personal data. To this extent the **Data Controller** determines the purposes for which and the means by which personal data are processed, while the **Data Processor** processes personal data only on behalf of the Data Controller.

Fenix and CINECA together can be considered as a joint Data Controller, this means they must jointly define 'why' and 'how' personal data should be processed. Joint Data Controllers must define an agreement setting out their respective responsibilities for complying with the GDPR rules. The main aspects of the agreement must be communicated to the individuals whose data is being processed, e.g. by mean of local site policies.

The supplier (as Data Processor⁶) processes personal data only on behalf of the Data Controller (Fenix and CINECA as part of the Fenix e-infrastructure). The supplier as Data Processor and CINECA/Fenix as Data Controller should also define together specific policies, describing for example what happens to the personal data once the present contract is terminated.

Moreover, the supplier may only sub-contract a part of its task to another Data Processor when it has received prior written authorisation from the Data Controller (CINECA/Fenix).

⁶ As Data Processor the supplier should comply with the GDPR and meet specific criteria: Article 28 of the EU GDPR "Processor"

CINECA/Fenix will elect also a Data Protection Officer (DPO)⁷. The DPO ensures, in an independent manner, that an organization applies the laws protecting individual personal data. The DPO will directly report to the highest management level in Fenix.

⁷ Articles 37,38 and 39 of the EU GDPR