



Finanziato
dall'Unione europea
NextGenerationEU



Ministero
dell'Università
e della Ricerca



Italiadomani
PIANO NAZIONALE
DI RIPRESA E RESILIENZA



Centro Nazionale di Ricerca in HPC,
Big Data and Quantum Computing

Enhancing Cloud Security with Integrated Information Management

Riccardo Rotondo

Workshop sul Calcolo nell'INFN La Biodola, 26-30 maggio 2025



Outline

- Context
- Requirements
- Technology
 - Freeipa and its components
 - Other services involved
- Implementation
 - Freeipa and Noggin portal features
 - Repository
- Conclusion
 - Current status
 - Future works
- References
- Acknowledgement



ICSC – Spoke 8 In silico medicine & Omics Data

- Big data analysis related to life science
- Clinical tests via simulation method
- Machine learning VS real experiment in labs
- Ad hoc therapy

Universal Immune System Simulator - UISS

- Use medical data
- Simulate & predict immune system response
- Model disease progression
- Find best therapy according immune system profiles



Università
di Catania

<https://pubmed.ncbi.nlm.nih.gov/32121606/>



UISS @ INFN Cloud: requirements



- **Data security**
 - ISO 9001 – 27001 Certified Server
 - Data managed according GDPR regulation
 - Restricted access to identified users
- **Network security**
 - Application secured by VPN
 - Two factor authentication
- **User Friendly**
- **Scalability**

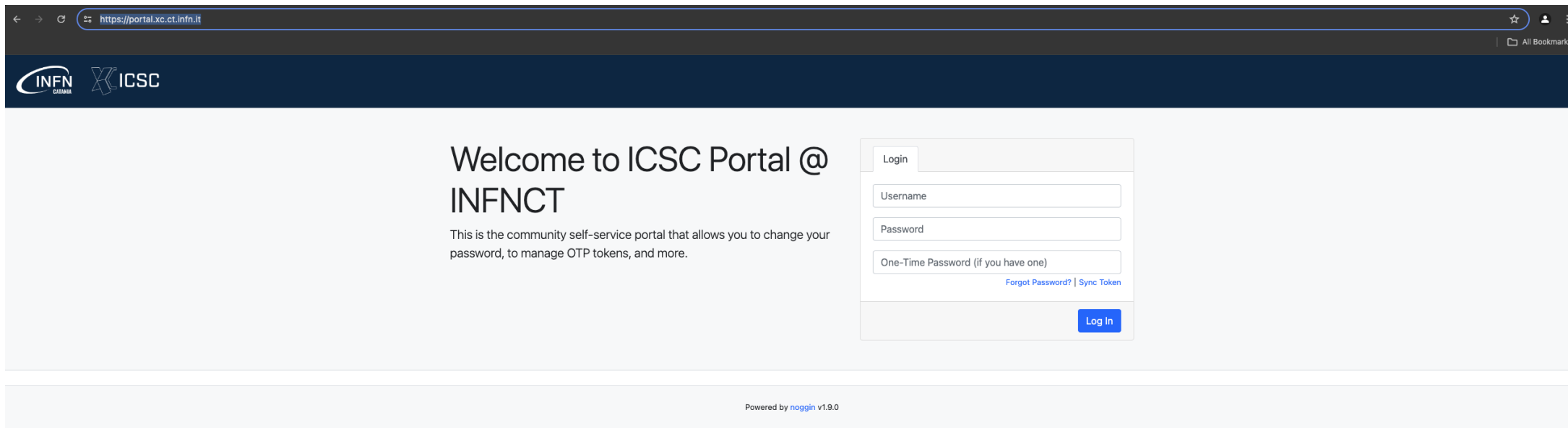


Integrated Security Management System: Freeipa

- Opensource
- 389 Directory Service (LDAP v3)
- MIT Kerberos KDC (Single-Sign-on)
- Dogtag Certificate System (CA)
- NTP
- SSSD
- Web UI and CLI
- Two factor authentication
- Released also in Container
- Used in EPIC for Identity management



Freeipa: first access to Noggin portal



The screenshot shows a web browser window with the address bar displaying <https://portal.xc.ct.infn.it>. The page header features the INFN and ICSC logos. The main content area has a heading "Welcome to ICSC Portal @ INFNCT" and a subtext: "This is the community self-service portal that allows you to change your password, to manage OTP tokens, and more." To the right is a login form with fields for "Username", "Password", and "One-Time Password (if you have one)". Below the password field are links for "Forgot Password?" and "Sync Token". A blue "Log In" button is at the bottom right of the form. The footer indicates "Powered by noggin v1.9.0".

Welcome to ICSC Portal @
INFNCT

This is the community self-service portal that allows you to change your password, to manage OTP tokens, and more.

Login

Username

Password

One-Time Password (if you have one)

[Forgot Password?](#) | [Sync Token](#)

Log In

Powered by [noggin](#) v1.9.0

<https://portal.xc.ct.infn.it>



Finanziato
dall'Unione europea
NextGenerationEU



Ministero
dell'Università
e della Ricerca



Italiadomani
PIANO NAZIONALE
DI RIPRESA E RESILIENZA



Freeipa: sign agreement and 2FA

portal.xc.ct.infn.it

INFN CATANIA X ICSC search... Groups

Settings for rotondo

Profile SSH & GPG Keys OTP Password Agreements

Disciplinare per l'uso delle risorse informatiche nell'INFN **Sign**

Powered by [noggin](#) v1.9.0
IPA server version 4.10.2. API version 2.252

portal.xc.ct.infn.it

INFN CATANIA X ICSC search... Groups

Settings for rotondo

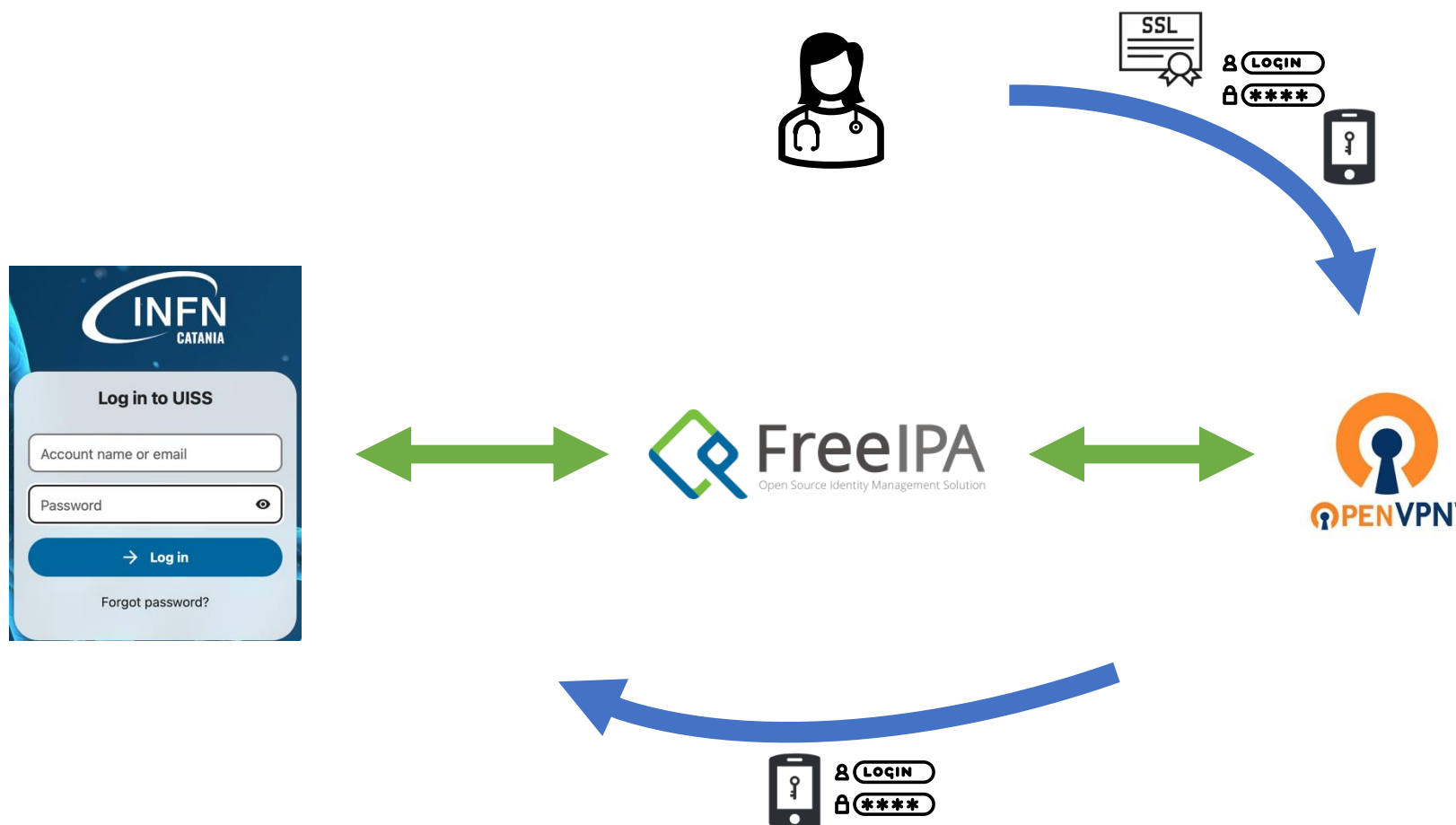
Profile Emails SSH & GPG Keys OTP Password Agreements

OTP Tokens **Add OTP Token**

bitwarden	Disable
freeotp	Disable

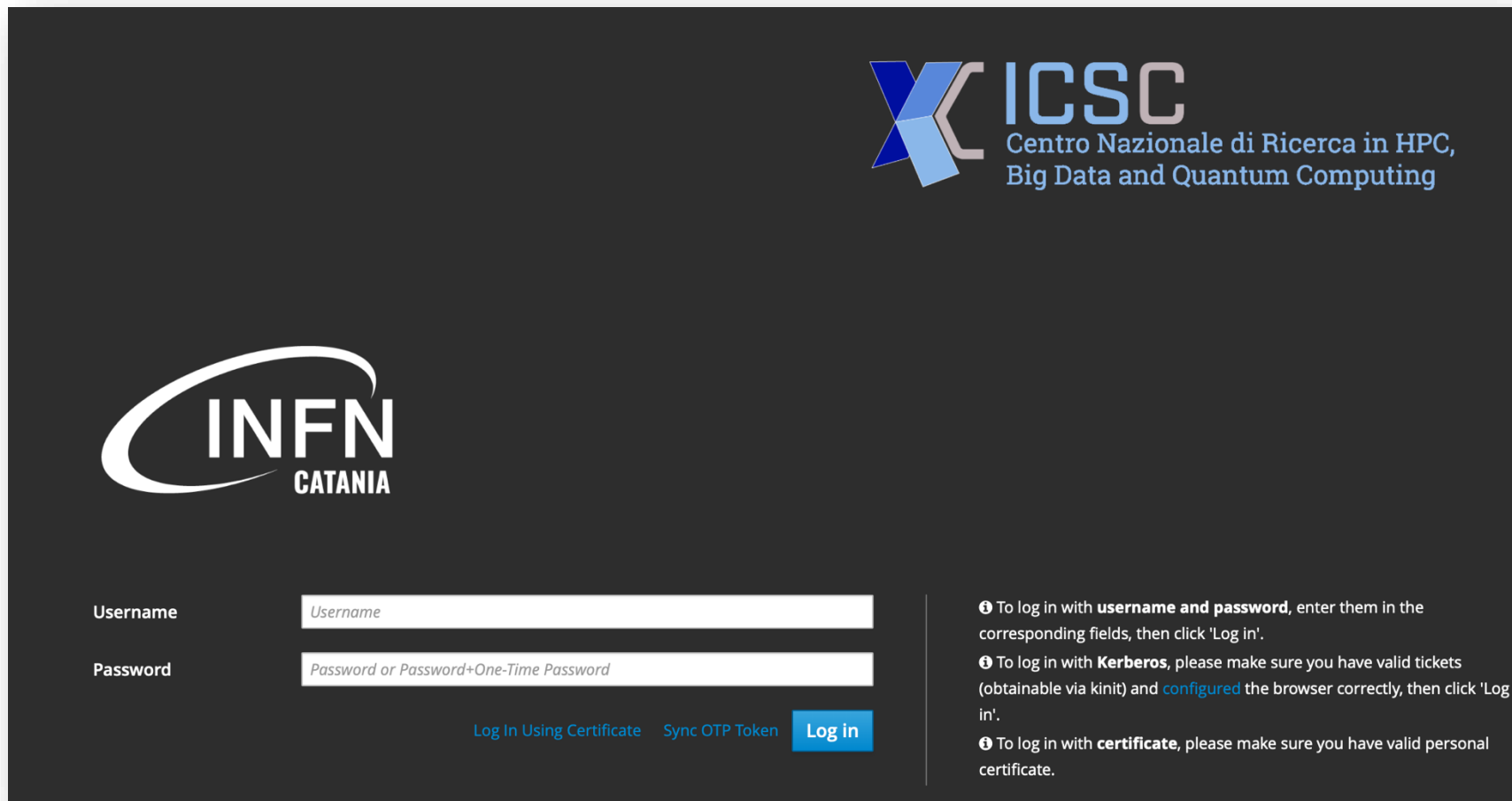
<https://portal.xc.ct.infn.it>

Freeipa: access to service provider by VPN



Freeipa: web UI

Freeipa internal
server



The image shows the FreeIPA web UI login page. It features a dark background with the ICSC logo in the top right corner. The ICSC logo consists of a stylized 'X' followed by 'ICSC' and the text 'Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing'. In the center, there is the INFN CATANIA logo, which includes a stylized 'C' and the text 'INFN CATANIA'. Below the logo, there are two input fields: 'Username' and 'Password'. The 'Username' field has a placeholder text 'Username'. The 'Password' field has a placeholder text 'Password or Password+One-Time Password'. Below the password field, there are three links: 'Log In Using Certificate', 'Sync OTP Token', and a blue 'Log in' button. To the right of the login fields, there are three informational paragraphs, each starting with an information icon (i) and a bolded keyword: 'username and password', 'Kerberos', and 'certificate'.

ICSC
Centro Nazionale di Ricerca in HPC,
Big Data and Quantum Computing

INFN
CATANIA

Username

Password

[Log In Using Certificate](#) [Sync OTP Token](#) [Log in](#)

i To log in with **username and password**, enter them in the corresponding fields, then click 'Log in'.

i To log in with **Kerberos**, please make sure you have valid tickets (obtainable via kinit) and **configured** the browser correctly, then click 'Log in'.

i To log in with **certificate**, please make sure you have valid personal certificate.

Freeipa: users, agreements, groups

INFN CATANIA

Identity Policy Authentication Network Services IPA Server

Users Hosts Services Groups ID Views Automember Subordinate IDs User Agreement

User categories

Active users

Stage users

Preserved users

Active users

Search

Refresh Delete Add Disable Enable Actions

<input type="checkbox"/>	User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
<input type="checkbox"/>								

INFN CATANIA

Identity Policy Authentication Network Services IPA Server

Users Hosts Services Groups ID Views Automember Subordinate IDs User Agreement

User Agreements

Search

Refresh Delete Add Disable Enable

<input type="checkbox"/>	Agreement name	Status	Agreement Description
<input type="checkbox"/>	Disciplinare per l'uso delle risorse informatiche nell'INFN	Enabled	Il presente disciplinare può essere scaricato all'indirizzo: https://l.infn.it/disciplinare-it Disciplinare per l'uso delle risorse informatiche nell'INFN 24 Gennaio 2020 1. PRINCIPI GENERALI L'Istituto Nazionale di Fisica Nucleare (INFN) è un ente pubblico nazionale di ricerca disciplinato dalle norme contenute nel proprio Statuto. L'INFN considera le risorse di calcolo ed i servizi di rete, nonché i dati e le informazioni da questi trattati, parte integrante del proprio patrimonio e funzionali al raggiungimento delle proprie finalità istituzionali di ricerca scientifica e tecnologica. Con il presente Disciplinare l'INFN intende salvaguardare la sicurezza del proprio sistema informatico e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati, anche personali, da questo prodotti, raccolti o comunque trattati. L'INFN, aderendo all'associazione Consortium GARR - Rete italiana dell'Università e della Ricerca - e utilizzandone i relativi servizi e strumenti, intende assicurare con il presente Disciplinare la conformità delle proprie norme con quelle dettate dal Consortium GARR. Nell'INFN il trattamento dei dati raccolti in relazione all'uso delle risorse di calcolo e dei servizi di rete avviene solo per finalità determinate, esplicite e legittime, nel rispetto dei principi di necessità, pertinenza, correttezza e non eccedenza secondo quanto previsto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. I sistemi informativi e i programmi informatici sono pertanto configurati in modo da ridurre al minimo l'utilizzo dei dati personali e identificativi. Tutti coloro ai quali è consentito l'accesso alle risorse di calcolo e ai servizi di rete sono tenuti al rispetto delle norme di seguito esposte, che

INFN CATANIA

Identity Policy Authentication Network Services IPA Server

Users Hosts Services Groups ID Views Automember Subordinate IDs User Agreement

User Groups > uiss

User Group: uiss

uiss members:

Users (5) User Groups Services External User ID over Show the previous page

uiss is a member of:

User Groups Netgroups Roles HBAC Rules Sudo Rules User Agreements (1) uiss member managers: User Groups Users


Refresh Delete Add

<input type="checkbox"/>	Agreement name
<input type="checkbox"/>	Disciplinare per l'uso delle risorse informatiche nell'INFN

Showing 1 to 1 of 1 entries.

Freeipa internal server

Freeipa: hosts, services



Administrator


IdentityPolicyAuthenticationNetwork ServicesIPA Server

UsersHostsServicesGroupsID ViewsAutomemberSubordinate IDs

User Agreement

Hosts

Search	Refresh	Delete	Add	Actions
Host name	Description	Enrolled		
<input type="checkbox"/> freeipa.		True		
<input type="checkbox"/> uiss.xc.				
<input type="checkbox"/> vpn.xc.		True		
Showing 1 to 3 of 3 entries.				



Administrator

IdentityPolicyAuthenticationNetwork ServicesIPA Server

UsersHostsServicesGroupsID ViewsAutomemberSubordinate IDs

User Agreement

Services

Search	Refresh	Delete	Add
Principal name			
<input type="checkbox"/> ...INFCT			
<input type="checkbox"/> ...INFCT			
<input type="checkbox"/> ...INFCT			
<input type="checkbox"/> ...INFCT			
<input type="checkbox"/> ...INFCT			
<input type="checkbox"/> ...INFCT			
<input type="checkbox"/> ...@XC.INFCT			
<input type="checkbox"/> ...INFCT			
<input type="checkbox"/> ...INFCT			
Showing 1 to 9 of 9 entries.			

Freeipa internal server

Freeipa container available on baltig

- Fork of official repo on baltig
- Add two customs image tag (fas_1.0, infnct_1.0):
 - Support to Noggin
 - Customise with INFNCT logo and colours
- Configuration guide:
 - Needs additional parameter in docker configuration
 - Docker volume proper configuration with right permission
 - Docker run parameters could lead to build failure

Services current status @ INFNCT

Service	Server	Docker Image	What for INFN Cloud
Noggin	Python VirtualEnv	Available on test branch	Test docker image
Freeipa	Virtual	Custom INFN Image created	Ready
VPN	Virtual	Not available	Prepare docker image or VM
Nextcloud	Physical	Available	Test docker image
UISS	Physical	Not Available	Prepare docker image or VM

Currently hosted @INFNCT (needs ISO 9001, 27001)



What for INFN Cloud

- EPIC certification (scheduled December 2025)
- Freeipa on Kubernetes:
 - Baltig repository
 - Manifest for service and pod
 - Custom rke2 configuration to meet freeipa container specifications
 - Still some disk permission issues to be fixed
- UISS on Kubernetes:
 - Container created and currently under test

Future works

Service	Server	Docker Image	What for INFN Cloud
Noggin	Virtual	Available on test branch	Test docker image
Freeipa (see next slide)	Virtual	Custom INFN Docker Image created	Test image on Kubernetes
VPN	Virtual	Not available	Prepare docker image or VM
New Web UI	Virtual	Not available	Prepare docker image or VM
UISS	Virtual	Docker Image created	Testing images



Conclusion

■ Limitation:

- Freeipa can interact with external IdP as OAuth 2.0 client[1]
- OAuth 2.0 client in Freeipa still presents issues because information cannot be easily shared with other clients[1]

■ Possible solutions:

- Keycloak (to be verified) [2]
- INFN IAM (when it will meet all requirements)

[1] <https://freeipa.readthedocs.io/en/latest/designs/external-idp/external-idp.html>

[2] <https://access.redhat.com/solutions/3010401>

Rereferences

- Noggin @ INFNCT: <https://portal.xc.ct.infn.it>
- Baltig:
 - Freeipa container: <https://baltig.infn.it/infnc/icsc/spoke8/freeipa-container>
 - INFNCT Noggin Theme: <https://baltig.infn.it/infnc/icsc/spoke8/infnc-noggin-theme>
 - Freeipa Kubernetes:
 - <https://baltig.infn.it/infnc/icsc/spoke8/freeipa-kubernetes>



Acknowledgment

- Salvatore Aurnia
- Valentina Ientile
- Barbara Martelli
- Salvatore Monforte



Centro Nazionale di Ricerca in HPC,
Big Data and Quantum Computing

*Supercomputing
shaping the future*